

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 3 1 日
Date of Application:

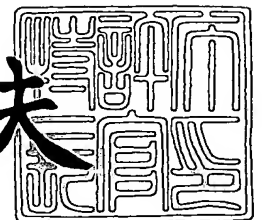
出 願 番 号 特 願 2 0 0 3 - 0 9 6 2 4 0
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 9 6 2 4 0]

出 願 人 株 式 会 社 リ コ ー
Applicant(s):

2 0 0 3 年 1 0 月 2 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 8 9 6 2 1

【書類名】 特許願

【整理番号】 0302583

【提出日】 平成15年 3月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G03G 21/00 396

【発明の名称】 情報処理装置とその情報管理システムおよびデジタル証明書取得方法並びにプログラム

【請求項の数】 21

【発明者】

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

【氏名】 小椋 正明

【特許出願人】

【識別番号】 000006747

【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号

【氏名又は名称】 株式会社リコー

【代表者】 桜井 正光

【代理人】

【識別番号】 100080931

【住所又は居所】 東京都豊島区東池袋 1 丁目 2 0 番 2 号 池袋ホワイトハウスビル 8 1 8 号

【弁理士】

【氏名又は名称】 大澤 敬

【手数料の表示】

【予納台帳番号】 014498

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809113

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置とその情報管理システムおよびデジタル証明書取得方法並びにプログラム

【特許請求の範囲】

【請求項 1】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知し、その識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置から該識別情報を含むデジタル証明書を受信した場合に、そのデジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませることを特徴とするデジタル証明書取得方法。

【請求項 2】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、前記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませることを特徴とするデジタル証明書取得方法。

【請求項 3】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受

信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、前記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませることを特徴とするデジタル証明書取得方法。

【請求項 4】 請求項 2 又は 3 記載のデジタル証明書取得方法において、
当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書をを用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化することを特徴とするデジタル証明書取得方法。

【請求項 5】 請求項 2 乃至 4 のいずれか一項に記載のデジタル証明書取得方法において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定することを特徴とするデジタル証明書取得方法。

【請求項 6】 請求項 2 乃至 4 のいずれか一項に記載のデジタル証明書取得方法において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除することを特徴とするデジタル証明書取得方法。

【請求項 7】 通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたことを特徴

とする情報処理装置。

【請求項 8】 通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、

情報を入力する入力手段と、

情報を記憶する記憶手段と、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、

該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、

前記生産台数分の通信装置の識別情報のいずれかが前記入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたことを特徴とする情報処理装置。

【請求項 9】 通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、

バーコードを読み取る読取手段と、

情報を記憶する記憶手段と、

前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、

該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、

前記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、

そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたことを特徴とする情報処理装置。

【請求項 10】 請求項 8 又は 9 記載の情報処理装置において、

前記デジタル証明書送信手段は、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書をを用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を有することを特徴とする情報処理装置。

【請求項 11】 請求項 8 乃至 10 のいずれか一項に記載の情報処理装置において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたことを特徴とする情報処理装置。

【請求項 12】 請求項 8 乃至 10 のいずれか一項に記載の情報処理装置において、

対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するデジタル証明書削除手段を設けたことを特徴とする情報処理装置。

【請求項 13】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、

前記情報処理装置に、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、

前記デジタル証明書管理装置に、前記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された識別情報を含むデジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成されたデジタル証明書を前記情報処理装置へ送信するデジタル証明書送信手段とを設けたことを特徴とする情報管理システム。

【請求項 14】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、

前記情報処理装置に、情報を入力する入力手段と、情報を記憶する記憶手段と、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、前記生産台数分の通信装置の識別情報のいずれかが前記入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、

前記デジタル証明書管理装置に、前記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を前記情報処理装置へ送信するデジタル証明書送信手段とを設けたことを特徴とする情報管理システム。

【請求項 15】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、

前記情報処理装置に、バーコードを読み取る読取手段と、情報を記憶する記憶手段と、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に

該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、前記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、

前記デジタル証明書管理装置に、前記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を前記情報処理装置へ送信するデジタル証明書送信手段とを設けたことを特徴とする情報管理システム。

【請求項 16】 請求項 14 又は 15 記載の情報管理システムにおいて、

前記情報処理装置のデジタル証明書送信手段は、当該情報処理装置の記憶手段から読み出したデジタル証明書に対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を有することを特徴とする情報管理システム。

【請求項 17】 請求項 14 乃至 16 のいずれか一項に記載の情報管理システムにおいて、

前記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたことを特徴とする情報管理システム。

【請求項 18】 請求項 14 乃至 16 のいずれか一項に記載の情報管理システムにおいて、

前記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から

削除するデジタル証明書削除手段を設けたことを特徴とする情報管理システム。

【請求項 1 9】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を前記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラム。

【請求項 2 0】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、前記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラム。

【請求項 2 1】 通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、前記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、前記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、前記生産台数分の通信装置のいずれ

かに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を前記デジタル証明書保存手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、この情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システム、および上記情報処理装置におけるデジタル証明書取得方法、並びに上記情報処理装置を制御するコンピュータに必要な機能（この発明に係わる機能）を実現させるためのプログラムに関する。

【0002】

【従来の技術】

従来から、通信機能を備えたプリンタ、ファクシミリ（FAX）装置、デジタル複写機、スキャナ装置、デジタル複合機等の画像処理装置を始め、ネットワーク家電、自動販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム等に通信機能（通信手段）を持たせた通信装置（電子装置）を被管理装置とし、サービスセンタ（管理センタ）の中央管理装置が公衆回線やインターネット等のネットワーク経由でこれらの被管理装置を遠隔管理する遠隔管理システムが提案されている。

【0003】

あるいは、被管理装置が通信機能を備えていない場合や、通信機能を備えていてもその機能が中央管理装置と通信するための機能を持っていない場合には、その被管理装置に中央管理装置と通信可能な通信機能を有する仲介装置をネットワーク経由で接続し、中央管理装置がネットワークおよび仲介装置経由で被管理装置を遠隔管理する遠隔管理システムも提案されている。

【0004】

一方、従来から、PC（パーソナルコンピュータ）等のコンピュータを複数台ネットワークを介して通信可能に接続し、少なくとも1台をサーバ装置（サーバ）、別の少なくとも1台をクライアント装置（クライアント）としたクライアント・サーバシステムを構成することが行われている。

このようなクライアント・サーバシステムにおいては、クライアント装置からサーバ装置に要求を送信し、サーバ装置がその要求に従った処理を行ってクライアント装置に対して応答を返す。

【0005】

したがって、上述した遠隔管理システムにおいて、通信装置あるいは通信装置が接続された仲介装置にクライアント装置の機能を、中央管理装置にサーバ装置の機能をそれぞれ持たせ、通信装置又は仲介装置をファイアウォールおよびネットワーク経由で中央管理装置と接続した場合には、通信装置又は仲介装置がポーリング（送信要求があるかどうかの問い合わせ）を中央管理装置に通知し、その中央管理装置がそのポーリングに従った処理を行って通信装置又は仲介装置に対して応答を返すことができる。

例えば、中央管理装置は、仲介装置からポーリングを受けると、課金カウンタ取得要求をその仲介装置へ通知する。

【0006】

ポーリング通知元の仲介装置は、中央管理装置から課金カウンタ取得要求を受けると、その課金カウンタ取得要求を自己に接続されている画像形成装置へ通知する。

その画像形成装置は、仲介装置から課金カウンタ取得要求を受けると、不揮発性メモリに格納されている課金カウンタのデータを読み取り、その読み取った課金カウンタのデータ（応答データ）を仲介装置へ送信する。

仲介装置は、画像形成装置から課金カウンタのデータを受信すると、それを中央管理装置へ送信する。

【0007】

このような場合においては、通信相手が適切か、あるいは送信される情報が改

ざんされていないかといった確認が重要である。また、特にインターネットにおいては、情報が通信相手に到達するまでに無関係なコンピュータを経由する場合が多いことから、機密データ（課金カウンタのデータ等）を送信する場合、その内容を盗み見られないようにする必要もある。そして、このような要求に応える通信プロトコルとして、例えばSSL（Secure Socket Layer）と呼ばれるプロトコルが開発されており、広く用いられている。このプロトコルを用いて通信を行うことにより、公開鍵暗号方式と共通鍵暗号方式とを組み合わせ、通信相手の認証を行うと共に、データの暗号化により改ざんおよび盗聴の防止を図ることができる。

【0008】

ここで、このSSLを用いて相互認証を行う場合の通信手順について、認証処理の部分に焦点を当てて説明する。

図24は、クライアント装置（通信装置又は仲介装置）とサーバ装置（仲介装置）とがSSLによる相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

図24に示すように、SSLによる相互認証を行う際には、まずクライアント装置側にルート鍵証明書、クライアント私有鍵、クライアント公開鍵証明書（クライアント証明書）を記憶させておく必要がある。クライアント私有鍵は、認証局（CA：certificate authority）がクライアント装置に対して発行した私有鍵である。そして、クライアント公開鍵証明書は、その私有鍵と対応する公開鍵にCAがデジタル署名を付してデジタル証明書としたものである。また、ルート鍵証明書は、CAがデジタル署名に用いた証明用私有鍵であるルート私有鍵と対応する証明用公開鍵（以下「証明鍵」ともいう）であるルート鍵に、デジタル署名を付してデジタル証明書としたものである。

【0009】

図25にこれらの関係を示す。

図25（a）に示すように、クライアント公開鍵は、クライアント私有鍵を用いて暗号化された文書を復号化するための鍵本体と、その公開鍵の発行者（CA）、発行相手（クライアント装置）、有効期限等の情報を含む書誌情報とによっ

て構成される。そして、CAは、鍵本体や書誌情報が改竄されていないことを示すため、クライアント公開鍵をハッシュ処理して得たハッシュ値を、ルート私有鍵を用いて暗号化し、デジタル署名としてクライアント公開鍵に付す。またこの際に、デジタル署名に用いるルート私有鍵の識別情報を署名鍵情報として公開鍵の書誌情報に加える。そして、このデジタル署名を付した公開鍵証明書が、クライアント公開鍵証明書である。

【0010】

このクライアント公開鍵証明書を認証処理に用いる場合には、ここに含まれるデジタル署名を、ルート私有鍵と対応する公開鍵であるルート鍵の鍵本体を用いて復号化する。この復号化が正常に行われれば、デジタル署名が確かにCAによって付されたことがわかる。また、クライアント公開鍵部分をハッシュ処理して得たハッシュ値と、復号して得たハッシュ値とが一致すれば、鍵自体も損傷や改竄を受けていないことがわかる。さらに、受信したデータをこのクライアント公開鍵を用いて正常に復号化できれば、そのデータは、クライアント私有鍵の持ち主、つまりクライアント装置から送信されたものであることがわかる。あとは、書誌情報を参照して、CAの信頼性やクライアント装置の登録有無等によって認証の正否を決定すればよい。

【0011】

ここで、認証を行うためには、ルート鍵を予め記憶しておく必要があるが、このルート鍵も、図25(b)に示すように、CAがデジタル署名を付したルート鍵証明書として記憶しておく。このルート鍵証明書は、自身に含まれる公開鍵でデジタル署名を復号化可能な、自己署名形式である。そして、ルート鍵を使用する際に、そのルート鍵証明書に含まれる鍵本体を用いてデジタル署名を復号化し、ルート鍵をハッシュ処理して得たハッシュ値と比較する。これが一致すれば、ルート鍵が破損等していないことを確認できるのである。

【0012】

図24の説明に戻ると、サーバ装置側には、ルート鍵証明書、サーバ私有鍵、サーバ公開鍵証明書（サーバ証明書）を記憶させておく必要がある。サーバ私有鍵及びサーバ公開鍵証明書は、CAがサーバ装置に対して発行した私有鍵及び公

開鍵証明書である。ここではクライアント装置とサーバ装置に対して同じCAが同じルート私有鍵を用いて証明書を発行しているものとし、この場合にはルート鍵証明書はクライアント装置とサーバ装置で共通となる。

【0013】

フローチャートの説明に入る。なお、図24において、2本のフローチャート間の矢印は、データの転送を示し、送信側は矢印の根元のステップで転送処理を行い、受信側はその情報を受信すると矢印の先端のステップの処理を行うものとする。また、各ステップの処理が正常に完了しなかった場合には、その時点で認証失敗の応答を返して処理を中断するものとする。相手から認証失敗の応答を受けた場合、処理がタイムアウトした場合等も同様である。

【0014】

クライアント・サーバシステムにおいて、接続を要求するのはクライアント装置側であるが、ユーザの指示等によってこの必要が生じた場合、クライアント装置のCPUは、所要の制御プログラムを実行することにより、図24の左側に示すフローチャートの処理を開始する。そして、ステップS11でサーバ装置に対して接続要求を送信する。

一方サーバ装置のCPUは、この接続要求を受信すると、所要の制御プログラムを実行することにより、図24の右側に示すフローチャートの処理を開始する。そして、ステップS21で第1の乱数を生成し、これをサーバ私有鍵を用いて暗号化する。そして、ステップS22でその暗号化した第1の乱数とサーバ公開鍵証明書とをクライアント装置に送信する。このステップS22の処理において、サーバ装置のCPUが第1のサーバ側認証処理手段として機能する。

【0015】

クライアント装置側では、これを受信すると、ステップS12でルート鍵証明書を用いてサーバ公開鍵証明書の正当性を確認する。これには、上述のように損傷や改竄を受けていないことを確認するのみならず、書誌情報を参照してサーバ装置が適当な通信相手であることを確認する処理を含む。

そして確認ができると、ステップS13で、受信したサーバ公開鍵証明書に含まれるサーバ公開鍵を用いて第1の乱数を復号化する。ここで復号化が成功すれ

ば、第1の乱数は確かにサーバ公開鍵証明書の発行対象であるサーバ装置から受信したものと確認できる。そして、サーバ装置を正当な通信相手として認証する。このステップS12及びS13の処理において、クライアント装置のCPUが第2のクライアント側認証処理手段として機能する。

【0016】

その後、ステップS14でこれとは別に第2の乱数及び第3の乱数を生成する。そして、ステップS15で第2の乱数をクライアント私有鍵を用いて暗号化し、第3の乱数をサーバ公開鍵を用いて暗号化し、ステップS16でこれらをクライアント公開鍵証明書と共にサーバ装置に送信する。第3の乱数の暗号化は、サーバ装置以外の装置に乱数を知られないようにするために行うものである。このステップS16の処理において、クライアント装置のCPUが第1のクライアント側認証処理手段として機能する。

【0017】

サーバ装置側では、これを受信すると、ステップS23でルート鍵証明書を用いてクライアント公開鍵証明書の正当性を確認する。これにも、ステップS12の場合と同様、クライアント装置が適当な通信相手であることを確認する処理を含む。そして確認ができると、ステップS24で、受信したクライアント公開鍵証明書に含まれるクライアント公開鍵を用いて第2の乱数を復号化する。ここで復号化が成功すれば、第2の乱数は確かにクライアント公開鍵証明書の発行対象であるクライアント装置から受信したものと確認できる。そして、サーバ装置を正当な通信相手として認証する。このステップS23及び24の処理において、サーバ装置のCPUが第2のサーバ側認証処理手段として機能する。

【0018】

その後、ステップS25でサーバ私有鍵を用いて第3の乱数を復号化する。ここまでの処理で、サーバ側とクライアント側に共通の第1乃至第3の乱数が共有されたことになる。そして、少なくとも第3の乱数は、生成したクライアント装置と、サーバ私有鍵を持つサーバ装置以外の装置が知ることはない。ここまでの処理が成功すると、ステップS26でクライアント装置に対して認証成功の応答を返す。

【0019】

クライアント装置側では、これを受信すると、ステップS17で第1乃至第3の乱数から共通鍵を生成し、以後の通信の暗号化に用いるものとして認証処理を終了する。サーバ装置側でも、ステップS27で同様の処理を行って終了する。そして、以上の処理によって互いに通信を確立し、以後はステップS17又はS27で生成した共通鍵を用い、共通鍵暗号方式でデータを暗号化して通信を行う。

このような処理を行うことにより、クライアント装置とサーバ装置が互いに相手を認証した上で安全に共通鍵を交換することができ、通信を確かな相手と安全に行うことができる。

【0020】

ところで、上述した遠隔管理システムにおいても、通信装置が、中央管理装置とSSLによる相互認証を行って通信可能にするためには、内部メモリ（記憶手段）にデジタル証明書（ルート鍵証明書、クライアント私有鍵、クライアント公開鍵証明書）を予め記憶（保存）させておく必要がある。デジタル証明書は、CA（認証局）から取得することができる。その取得に関しては、例えば特許文献1に記載されている。また、通信装置の販売会社と保守契約をする必要があり、それによって中央管理装置による遠隔管理が可能になる。

【0021】

【特許文献1】

特開2001-325249号公報

【0022】

【発明が解決しようとする課題】

遠隔管理システムに使用される通信装置は、毎日、機種毎に決定された台数分だけ生産されるようになっており、その機種毎に内部メモリにデジタル証明書を記憶させるかどうか、つまり中央管理装置による遠隔管理に対応できるかどうかも決定される。注文生産されるものではないため、保守契約後、内部メモリにデジタル証明書を記憶した通信装置を生産する、ということとはできない。

よって、機種によっては、保守契約をしていなくても、内部メモリにデジタル

証明書を記憶した通信装置は当然存在するため、その通信装置を保守契約した通信装置とし、管理装置によって遠隔管理されるようにすることも可能である。

【0023】

例えば、2台の通信装置を所有する機器利用者が、保守契約している通信装置の課金カウンタの値より保守契約していない通信装置の課金カウンタの値が小さいような場合、後者の通信装置の方が保守料金が安く済むため、その通信装置を前者の通信装置とし、課金カウンタの値を示すカウンタ情報を中央管理装置へ送信することも可能である。その場合、中央管理装置側では、後者の通信装置から受信したカウンタ情報に基づいて保守料金を計算するため、その保守料金、つまり安い方の保守料金を機器利用者に請求することになる。

【0024】

この発明は、上記の問題点に鑑みてなされたものであり、中央管理装置側が、通信装置と通信する際の認証時に、その通信装置が保守契約したものであるかどうかを正確に判定できるようにすることを目的とする。

【0025】

【課題を解決するための手段】

この発明は、上記の目的を達成するため、情報処理装置、情報管理システム、および上記情報処理装置におけるデジタル証明書取得方法、並びに上記情報処理装置を制御するコンピュータに必要な機能を実現させるためのプログラムを提供する。

【0026】

請求項1の発明によるデジタル証明書取得方法は、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知し、その識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置から該識別情報を含むデジタル証明書を受信した場合に、そのデジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるものである。

【0027】

請求項2の発明によるデジタル証明書取得方法は、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、上記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるものである。

【0028】

請求項3の発明によるデジタル証明書取得方法は、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置におけるデジタル証明書取得方法において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知し、その各識別情報を付加したデジタル証明書の要求通知に対して、該デジタル証明書管理装置からその各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存した後、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を該記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるものである。

【0029】

請求項4の発明によるデジタル証明書取得方法は、請求項2又は3のデジタル証明書取得方法において、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書

を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化するものである。

請求項 5 の発明によるデジタル証明書取得方法は、請求項 2 ～ 4 のいずれかのデジタル証明書取得方法において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定するものである。

請求項 6 の発明によるデジタル証明書取得方法は、請求項 2 ～ 4 のいずれかのデジタル証明書取得方法において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するものである。

【0030】

請求項 7 の発明による情報処理装置は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたものである。

【0031】

請求項 8 の発明による情報処理装置は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、情報を入力する入力手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、上記生産台数分の通信装置の識別情報のいずれかが上記

入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたものである。

【0032】

請求項9の発明による情報処理装置は、通信装置に所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置において、バーコードを読み取る読取手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設けたものである。

【0033】

請求項10の発明による情報処理装置は、請求項8又は9の情報処理装置において、上記デジタル証明書送信手段に、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を備えたものである。

請求項11の発明による情報処理装置は、請求項8～10のいずれかの情報処理装置において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたものである。

請求項12の発明による情報処理装置は、請求項8～10のいずれかの情報処

理装置において、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するデジタル証明書削除手段を設けたものである。

【0034】

請求項13の発明による情報管理システムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、上記情報処理装置に、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、上記デジタル証明書管理装置に、上記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された識別情報を含むデジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成されたデジタル証明書を上記情報処理装置へ送信するデジタル証明書送信手段とを設けたものである。

【0035】

請求項14の発明による情報管理システムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、上記情報処理装置に、情報を入力する入力手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と

、上記生産台数分の通信装置の識別情報のいずれかが上記入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、上記デジタル証明書管理装置に、上記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を上記情報処理装置へ送信するデジタル証明書送信手段とを設けたものである。

【 0 0 3 6 】

請求項 1 5 の発明による情報管理システムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置と、該情報処理装置とネットワークを介して通信可能なデジタル証明書管理装置とからなる情報管理システムにおいて、上記情報処理装置に、バーコードを読み取る読取手段と、情報を記憶する記憶手段と、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求手段と、該手段による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存手段と、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信手段とを設け、上記デジタル証明書管理装置に、上記機器管理装置からデジタル証明書の送信要求を受けた場合に、該送信要求に付加された各識別情報をそれぞれ含む各デジタル証明書を生成するデジタル証明書生成手段と、該手段によって生成された各デジタル証明書を上記情報処理装置へ送信するデジタル証明書送信手段とを設けたものである。

【0037】

請求項16の発明による情報管理システムは、請求項14又は15の情報管理システムにおいて、上記情報処理装置のデジタル証明書送信手段に、当該情報処理装置の記憶手段から読み出したデジタル証明書を対応する通信装置へ送信する際に、該通信装置との間でデジタル証明書を用いて認証を行い、該記憶手段から読み出したデジタル証明書を暗号化する手段を備えたものである。

請求項17の発明による情報管理システムは、請求項14～16のいずれかの情報管理システムにおいて、上記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書の書き込み済みを示す情報を設定する書き込み済み情報設定手段を設けたものである。

請求項18の発明による情報管理システムは、請求項14～16のいずれかの情報管理システムにおいて、上記情報処理装置に、対応する通信装置の記憶手段へのデジタル証明書の書き込みが完了した場合に、そのデジタル証明書を当該情報処理装置の記憶手段から削除するデジタル証明書削除手段を設けたものである。

【0038】

請求項19の発明によるプログラムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、該各デジタル証明書を上記通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラムである。

【0039】

請求項20の発明によるプログラムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の

識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、上記生産台数分の通信装置の識別情報のいずれかが入力手段によって入力された場合に、その識別情報に対応するデジタル証明書を当該情報処理装置の記憶手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラムである。

【0040】

請求項21の発明によるプログラムは、通信装置へ所要の情報を送信して該通信装置の記憶手段に書き込ませる情報処理装置を制御するコンピュータに、上記通信装置による通信時の認証に用いるデジタル証明書の送信要求に該通信装置の識別情報を該通信装置の生産台数分だけ付加してデジタル証明書管理装置へ通知するデジタル証明書送信要求機能と、該機能による各識別情報を付加したデジタル証明書の送信要求に対して、上記デジタル証明書管理装置から該各識別情報をそれぞれ含む各デジタル証明書を受信した場合に、その各デジタル証明書を当該情報処理装置の記憶手段に保存するデジタル証明書保存機能と、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の識別情報を示すバーコードが読取手段によって読み取られ、そのバーコードによる識別情報が入力された場合に、その識別情報に対応するデジタル証明書を上記デジタル証明書保存手段から読み出して対応する通信装置へ送信して該通信装置の記憶手段に書き込ませるデジタル証明書送信機能とを実現させるためのプログラムである。

【0041】

【発明の実施の形態】

以下、この発明の好ましい実施の形態を図面を参照して説明する。

まず、この発明による通信装置を被管理装置とする遠隔管理システムの構成例について説明する。図1は、その遠隔管理システムの構成の一例を示す概念図で

ある。

【0042】

この遠隔管理システムは、プリンタ、FAX装置、デジタル複写機、スキャナ装置、デジタル複合機等の画像処理装置や、ネットワーク家電、自動販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム等に通信機能を持たせた通信装置（電子装置）を被管理装置10（10a, 10b, 10c, 10d, 10e, 10f）とする遠隔管理システムである。そして、この被管理装置10と接続される（被管理装置側から見た）外部装置として、被管理装置10とLAN（ローカルエリアネットワーク）によって接続された遠隔管理仲介装置である仲介装置101（101a, 101b, 101c）、更に仲介装置101とインターネット103（公衆回線等の他のネットワークでもよい）を介して接続されるサーバ装置として機能する中央管理装置（以下単に「管理装置」ともいう）102を備え、当該中央管理装置102が、仲介装置101を介して各被管理装置10を集中的に遠隔管理できるようにしたものである。当該仲介装置101および被管理装置10は、その利用環境に応じて多様な階層構造を成す。

【0043】

例えば、図1に示す設置環境Aでは、中央管理装置102とHTTP（Hyper Text Transfer Protocol）による直接的なコネクションを確立できる仲介装置101aが、被管理装置10a及び10bを従える単純な階層構造になっているが、同図に示す設置環境Bでは、4台の被管理装置10を設置するため、1台の仲介装置101を設置しただけでは負荷が大きくなる。そのため、中央管理装置102とHTTPによる直接的なコネクションを確立できる仲介装置101bが、被管理装置10cおよび10dだけでなく、他の仲介装置101cを従え、この仲介装置101cが被管理装置10eおよび10fを更に従えるという階層構造を形成している。この場合、被管理装置10eおよび10fを遠隔管理するために中央管理装置102から発せられた情報は、仲介装置101bとその下位のノードである仲介装置101cとを經由して、被管理装置10e又は10fに到達することになる。

【0044】

また、設置環境Cのように、被管理装置10に仲介装置101の機能を併せ持たせた仲介機能付被管理装置（以下単に「被管理装置」ともいう）11a, 11bを、別途仲介装置を介さずにインターネット103によって中央管理装置102に接続するようにしてもよい。

図示はしていないが、仲介機能付被管理装置11の下位に更に被管理装置10と同等の被管理装置を接続することもできる。

なお、各設置環境A, B, Cには、セキュリティ面を考慮し、ファイアウォール104を設置する。

また、この遠隔管理システムにおいては、サービスセンタSの中央管理装置102に、後述する生産工場Eの通信端末150が接続されている。

【0045】

このような遠隔管理システムにおいて、仲介装置101は、これに接続された被管理装置10の制御管理のためのアプリケーションプログラムを実装している。

中央管理装置102は、各仲介装置101の制御管理、更にはこの仲介装置101を介した被管理装置10の制御管理を行うためのアプリケーションプログラムを実装している。そして、被管理装置10も含め、この遠隔管理システムにおけるこれら各ノードは、RPC (remote procedure call) により、相互の実装するアプリケーションプログラムのメソッドに対する処理の依頼である「要求」を送信し、この依頼された処理の結果である「応答」を取得することができるようになっている。

【0046】

すなわち、仲介装置101又はこれと接続された被管理装置10では、中央管理装置102への要求を生成してこれを中央管理装置102へ引き渡し、この要求に対する応答を取得できる一方で、中央管理装置102は、上記仲介装置101側への要求を生成してこれを仲介装置101側へ引き渡し、この要求に対する応答を取得できるようになっている。この要求には、仲介装置101に被管理装置10に対して各種要求を送信させ、被管理装置10からの応答を仲介装置101を介して取得することも含まれる。

なお、RPCを実現するために、SOAP (Simple Object Access Protocol) , HTTP, FTP (File Transfer Protocol) , COM (Component Object Model) , CORBA (Common Object Request Broker Architecture) 等の既知のプロトコル (通信規格) , 技術, 仕様などを利用することができる。

【0047】

この送受信のデータ送受モデルを図2の概念図に示す。

(A) は、被管理装置10で中央管理装置102に対する要求が発生したケースである。このケースでは、被管理装置10が被管理装置側要求aを生成し、これを仲介装置101を経由して受け取った中央管理装置102がこの要求に対する応答aを返すというモデルになる。同図に示す仲介装置101は複数であるケースも想定できる (上記図1に示す設置環境B)。なお、(A) では、応答aだけでなく応答遅延通知a'を返信するケースが表記されている。これは、中央管理装置102を、仲介装置101を経由して被管理装置側要求を受け取って、当該要求に対する応答を即座に返せないと判断したときには、応答遅延通知を通知して一旦接続状態を切断し、次の接続の際に上記要求に対する応答を改めて引き渡す構成としているためである。

【0048】

(B) は、中央管理装置102で被管理装置10に対する要求が発生したケースである。このケースでは、中央管理装置102が管理装置側要求bを生成し、これを仲介装置101を経由して受け取った被管理装置10が、当該要求に対する応答bを返すというモデルになっている。なお、(B) のケースでも、応答を即座に返せないときに応答遅延通知b'を返すことは(A) のケースと同様である。

【0049】

次に、図1に示す中央管理装置102の物理的構成について簡単に説明すると、当該中央管理装置102は、CPU, ROM, RAM等からなる制御装置や、データベース、モデム、プロシキサーバ等によって構成されている。その構成については、追って詳細に説明する。

さらに、図1に示す仲介装置101の物理的構成について説明すると、当該仲

介装置 101 は、不図示の CPU, ROM, RAM, 不揮発性メモリ, ネットワークインタフェースカード (NIC) 等によって構成されている。

また、仲介機能付被管理装置 11 については、仲介装置 101 の機能を実現するためにこれらのユニットを単に被管理装置 10 に付加しても良いが、被管理装置 10 に備える CPU, ROM, RAM 等のハードウェア資源を利用し、CPU に適当なアプリケーションやプログラムモジュールを実行させることによって仲介装置 101 の機能を実現することもできる。

【0050】

以下、図 1 に示した遠隔管理システムのより具体的な例として、この発明による通信装置である画像形成装置を被管理装置とした、この発明による通信装置の遠隔管理システムである画像形成装置遠隔管理システムについて説明する。図 3 は、その画像形成装置遠隔管理システムの構成の一例を示す概念図であるが、被管理装置 10 を画像形成装置 100 に、仲介機能付被管理装置 11 を仲介機能付画像形成装置（以下単に「画像形成装置」ともいう）110 に変更した点が図 1 と相違するのみであるので、システムの全体構成についての説明は省略する。

画像形成装置 100 は、コピー、ファクシミリ、スキャナ等の機能および外部装置と通信を行う機能を備えたデジタル複合機であり、それらの機能に係るサービスを提供するためのアプリケーションプログラムを実装しているものである。また、仲介機能付画像形成装置 110 は、画像形成装置 100 に仲介装置 101 の機能を併せ持たせたものである。

【0051】

このような画像形成装置 100 の物理的構成について図 4 を用いて説明する。

図 4 は、画像形成装置 100 内のハードウェア構成例を示すブロック図である。図 5 はフラッシュメモリ 204 の記憶エリアの構成例を、図 6 は NV RAM 207 の記憶エリアの構成例をそれぞれ示すメモリマップ図である。

この画像形成装置 100 は、CPU 201, ASIC (Application Specific Integrated Circuit) 202, SDRAM 203, フラッシュメモリ (不揮発性メモリ) 204, NRS 用メモリ 205, PHY (物理メディアインタフェース) 206, NV-RAM (不揮発性メモリ) 207, 操作部 209, HDD (

ハードディスクドライブ) 210, モデム 211, P I (パーソナルインタフェース) 212, F C U (ファックスコントロールユニット) 213, U S B (Universal Serial Bus) 214, I E E E 1394 215, L P (読み取り・書き込み部) 216, および周辺機 217 を備えている。

【0052】

C P U 201 は、A S I C 202 を介してデータ処理 (各機能の制御) を行う演算処理手段である。

A S I C 202 は、C P U インターフェース, S D R A M インターフェース, ローカルバスインターフェース, P C I インターフェース, M A C (Media Access Controller)、H D D インターフェースなどからなる多機能デバイスボードであり、C P U 201 の制御対象となるデバイスの共有化を図り、アーキテクチャの面からアプリ (アプリケーションソフト) や共通システムサービスの開発の高効率化を支援するものである。

S D R A M 203 は、O S を含む各種プログラムを記憶するプログラムメモリや、C P U 201 がデータ処理を行う際に使用するワークメモリ等として使用するメインメモリである。なお、この S D R A M 203 の代わりに、D R A M や S R A M を使用してもよい。

【0053】

フラッシュメモリ 204 は、例えば図 5 に示すように、この画像形成装置 100 を起動させるブートローダ (ブートプログラム) や O S のファイルである O S イメージを記憶するプログラムメモリ、中央管理装置 102 との通信時の S S L による相互認証に用いるデジタル証明書 (以下単に「証明書」ともいう) を記憶する証明書メモリ、各サービス実現のための通信時の S S L による相互認証に用いる共通のデジタル証明書 (以下単に「共通証明書」ともいう) を記憶する共通証明書メモリ、種々の固定パラメータを記憶する固定パラメータメモリ等として使用する不揮発性メモリ (記憶手段) であり、電源がオフになっても記憶内容を保持するようになっている。なお、このフラッシュメモリ 204 の代わりに、R A M と電池を利用したバックアップ回路を集積した不揮発性 R A M や、E E P R O M 等の他の不揮発性メモリを使用してもよい。

【0054】

NRS用メモリ205は、後述するNRSを記憶する不揮発性メモリであり、オプションでNRS機能を追加することができる。

PHY206は、LANを介して外部装置と通信を行うためのインタフェースである。

NVRAM207は、例えば図6に示すように、この画像形成装置100の識別情報である機種機番を記憶する機種機番メモリ、操作部209による操作上の初期値を記憶するメモリ、各アプリ（APL）の初期値を記憶するメモリ、各カウンタ情報（課金カウンタのデータ）を記憶するメモリ、上述した共通証明書を記憶する共通証明書メモリ等として使用する不揮発性メモリ（記憶手段）であり、電源がオフになっても記憶内容を保持するようになっている。なお、このNVRAM207として、RAMと電池を利用したバックアップ回路を集積した不揮発性RAMや、EEPROM、フラッシュメモリ等の不揮発性メモリを使用することができる。

【0055】

操作部209は、操作表示手段（操作手段および表示手段）である。

HDD210は、電源のオン・オフに関係なくデータを記憶保存する記憶手段（記録媒体）である。このHDD210に、上述したフラッシュメモリ204内のプログラムやそれ以外のデータ、あるいはNVRAM207内のデータを記憶しておくこともできる。

モデム211は、変復調手段であり、中央管理装置102へ公衆回線経由でデータを送信する場合、そのデータを公衆回線に流せる形に変調する。また、管理装置102から送られてくる変調されたデータを受信した場合、そのデータを復調する。

【0056】

PI212は、RS485規格に準拠したインタフェースを備え、図示しないラインアダプタを介して公衆回線に接続している。

FCU213は、FAX装置又はモデム機能（FAX通信機能）を有するデジタル複写機やデジタル複合機等の画像形成装置および中央管理装置102等の外

部装置との通信を公衆回線経由で制御する。

ここで、電源投入（電源オン）により、CPU201は、ASIC202経由でフラッシュメモリ204内のブートローダを起動させ、そのブートローダに従い、フラッシュメモリ204内のOSイメージを読み出し、それをSDRAM203にロードして使用可能なOSに展開する。そして、OSの展開が完了すると、そのOSを起動させる。その後、必要に応じてフラッシュメモリ204内のアプリ等のプログラムあるいはNRS用メモリ205内のNRSを読み出し、それをSDRAM203にロードして展開し、起動させることにより、各種機能を実現することができる。

【0057】

次に、画像形成装置100（又は110）におけるソフトウェア構成を図7を用いて説明する。

図7は、画像形成装置100のソフトウェア構成の一例を示すブロック図である。当該画像形成装置100のソフトウェア構成は、最上位のアプリケーションモジュール層、その下位のサービスモジュール層からなる。そして、これらのソフトウェアを構成するプログラムはフラッシュメモリ204やNRS用メモリ205に記憶され、必要に応じて読み出されてCPU201によって実行される。

【0058】

アプリケーションモジュール層のソフトウェアは、CPU201を、ハードウェア資源を動作させて所定の機能を実現させる複数のアプリケーション制御手段（処理実行手段）として機能させるためのプログラムによって構成され、サービスモジュール層のソフトウェアは、CPUを、ハードウェア資源と各アプリケーション制御手段との間に介在し、複数のアプリケーション制御手段からのハードウェア資源に対する動作要求の受付、その動作要求の調停、およびその動作要求に基づく動作の実行制御を行うサービス制御手段（処理実行手段）として機能させるためのプログラムによって構成される。

【0059】

なお、それらの機能のうち、中央管理装置102との通信に係わる機能（通信手段としての機能）の実現方法は、画像形成装置100と画像形成装置110と

によって異なる。つまり、画像形成装置 110 の場合は、仲介装置 101 の機能を備えているため、CPU が対応するプログラムを実行することにより、中央管理装置 102 との通信に係わる機能を実現することができる。画像形成装置 100 の場合には、CPU が対応するプログラムを実行すると共に、仲介装置 101 を利用することにより、中央管理装置 102 との通信に係わる機能を実現することができる。

【0060】

サービスモジュール層には、オペレーションコントロールサービス (OCS) 300、エンジンコントロールサービス (ECS) 301、メモリコントロールサービス (MCS) 302、ネットワークコントロールサービス (NCS) 303、ファクスコントロールサービス (FCS) 304、ニューリモートサービス (NRS) 305、システムコントロールサービス (SCS) 306、システムリソースマネージャ (SRM) 307、イメージメモリハンドラ (IMH) 308、カスタマーサポートシステム (CSS) 315、デリバリーコントロールサービス (DCS) 316、ユーザコントロールサービス (UCS) 317 を実装している。更に、アプリケーションモジュール層には、コピーアプリ 309、ファクスアプリ 310、プリンタアプリ 311、スキャナアプリ 312、ネットファイルアプリ 313、ウェブアプリ 314 を実装している。

【0061】

これらを更に詳述する。

OCS 300 は、操作部 209 を制御するモジュールである。

ECS 301 は、ハードウェアリソース等のエンジンを制御するモジュールである。

MCS 302 は、メモリ制御をするモジュールであり、例えば、画像メモリの取得及び開放、HDD 201 の利用等を行う。

NCS 303 は、ネットワークとアプリケーションモジュール層の各アプリケーションプログラムとの仲介処理を行わせるモジュールである。

FCS 304 は、ファクシミリ送受信、ファクシミリ読み取り、ファクシミリ受信印刷等を行うモジュールである。

【0062】

NRS305は、ネットワークを介してデータを送受信する際のデータの変換等をするモジュールであり、またネットワークを介した遠隔管理に関する機能（中央管理装置102との通信に係わる機能）をまとめたモジュールである。

SCS306は、コマンドの内容に応じたアプリケーションモジュール層の各アプリケーションプログラムの起動管理及び終了管理を行うモジュールである。

SRM307は、システムの制御及びリソースの管理を行うモジュールである。

IMH308は、一時的に画像データを入れておくメモリを管理するモジュールである。

【0063】

CSS315は、公衆回線を介してデータを送受信する際のデータの変換等をするモジュールであり、また公衆回線を介した遠隔管理に関する機能をまとめたモジュールである。

DCS316は、HDD210やSDRAM203に記憶している（する）画像ファイル等をSMTP（Simple Mail Transfer Protocol）やFTP（File Transfer Protocol）を用いて送受信するモジュールである。

UCS317は、ユーザが登録した宛先情報や宛名情報等のユーザ情報を管理するモジュールである。

【0064】

コピーアプリ309は、コピーサービスを実現するためのアプリケーションプログラムである。

ファクスアプリ310は、ファクスサービスを実現するためのアプリケーションプログラムである。

プリンタアプリ311は、プリンタサービスを実現するためのアプリケーションプログラムである。

【0065】

スキャナアプリ312は、スキャナサービスを実現するためのアプリケーションプログラムである。

ネットファイルアプリ 313 は、ネットファイルサービスを実現するためのアプリケーションプログラムである。

ウェブアプリ 314 は、ウェブサービスを実現するためのアプリケーションプログラムである。

【0066】

次に、上述した画像形成装置 100 のソフトウェアの構成に含まれる NRS モジュールの内部構成を図 8 を用いて更に説明する。

図 8 は、NRS モジュールの構成の一例を示す機能ブロック図である。同図に示すように、NRS 305 は、SCS 306 と NCS 303 との間で処理をおこなっている。ウェブサーバ機能部 500 は、外部から受信した要求に関する応答処理を行う。ここでの要求は、例えば、構造化言語である XML (Extensible Markup Language) 形式で記載された、SOAP (Simple Object Access Protocol) による SOAP リクエストであることが考えられる。ウェブクライアント機能部 501 は、外部への要求を発行する処理を行う。libsoap 502 は、SOAP を処理するライブラリであり、libxml 503 は、XML 形式で記載されたデータを処理するライブラリである。また、libgwww 504 は、HTTP を処理するライブラリであり、libgw_ncs 505 は、NCS 303 との間の処理をするライブラリである。

【0067】

図 9 は、中央管理装置 102 内の物理的構成例を示すブロック図である。

この中央管理装置 102 は、モデム 601、通信端末 602、プロキシ (Proxy) サーバ 603、操作者端末 604、外部接続 I/F 605、ファイルサーバ 606、デジタル証明書管理装置 (以下単に「証明書管理装置」ともいう) 607、制御装置 608 等からなる。

モデム 601 は、図示しない公衆回線を介して機器利用者側 (例えば画像形成装置を利用しているユーザ先) の仲介装置 101 又は画像形成装置 110 と通信するものであり、送受信するデータを変復調する。このモデム 601 と後述する通信端末 602 により通信手段としての機能を果たす。

【0068】

通信端末 602 は、モデム 601 による通信を制御するものである。

プロキシサーバ 603 は、インターネット 103 を介して機器利用者側の仲介装置 101 又は画像形成装置 110 との通信およびセキュリティ管理を行う。このプロキシサーバ 603 も、通信手段としての機能を果たす。

操作者端末 604 は、各種データの入力をオペレータによるキーボード等の入力装置上の操作により受け付ける。入力されるデータとしては、例えば、各機器利用者側の仲介装置 101 又は画像形成装置 110 と通信する際に使用するそれらの IP アドレスや電話番号（発呼先電話番号）等の顧客情報がある。

【0069】

外部接続 I/F 605 は、図 3 の生産工場 E 内の通信端末 150 と接続するためのインタフェースである。

ファイルサーバ 606 は、図示しないハードディスク装置等の記憶装置を備え、そこに各機器利用者側の仲介装置 101 および画像形成装置 110 の IP アドレスや電話番号、それらの装置から受信したデータ、操作者端末 604 から入力されたデータ、およびこの発明に係わるプログラム等の各種データをそれぞれデータベース（DB）として記憶している。

【0070】

証明書管理装置 607 は、生産工場 E 内の通信端末 150 からの送信要求により、上述した証明書や共通証明書を発行し、それを中央管理装置 102 へ送信するものである。これについては、追って詳細に説明する。

制御装置 608 は、図示しない CPU、ROM、RAM 等からなるマイクロコンピュータを備えており、中央管理装置 102 全体を統括的に制御する。その CPU が、上記プログラムに従って動作する（上記プログラムを必要に応じて実行する）と共に、モデム 601、通信端末 602、又はプロキシサーバ 603 を必要に応じて選択的に使用することにより、各種処理を行うことができる。

【0071】

図 10 は、図 3 の生産工場 E の内部構成例を示すブロック図である。

この生産工場 E には、生産管理システム 140、通信端末 150、工場端末 160 が設置されている。

生産管理システム 140 は、画像形成装置 100, 110, 仲介装置 101 等の通信装置（又はそれらの通信装置に設けられる制御基板）の日々の生産台数を管理する。

通信端末 150 は、生産管理システム 140 からその日の通信装置の機種機番（機種コードとシリアル番号とを含めた情報）別の生産台数を入手（取得）し、その情報に基づいて中央管理装置 102 内の証明書管理装置 607（認証局に相当する）から必要な証明書を入手する。

【0072】

工場端末 160 は、バーコードリーダ 141 によって読み取られたバーコードによる機種機番が入力された場合に、その機種機番に対応する証明書を通信端末 150 から入手し、それを対応する通信装置へ送信してその通信装置の不揮発性メモリ（記憶手段）に書き込ませる。

ここで、通信端末 150 および工場端末 160 により、この発明による情報処理装置を構成する。

バーコードリーダ 141 は、読取手段であり、通信装置に貼付された定格銘板あるいは対応するチェックシート上の機種機番（識別情報）を示すバーコードの情報を読み取って工場端末 160 へ送信する。このバーコードリーダ 141 として、ハンドタイプの小型バーコードリーダがある。

【0073】

図 11 は、証明書管理装置 607 のハードウェア構成例を示すブロック図である。

証明書管理装置 607 は、CPU 131, ROM 132, RAM 133（記憶手段）, HDD 134（記憶手段）, 通信 I/F 135 を備え、これらがシステムバス 136 によって接続されている。

この証明書管理装置 607 によれば、CPU 131 が ROM 132 や HDD 134 に記憶されている各種制御プログラムを実行することによってこの証明書管理装置 607 の動作を制御し、この発明による機能（デジタル証明書生成手段、デジタル証明書送信手段としての機能）を実現することができる。

【0074】

図12は、通信端末150のハードウェア構成例を示すブロック図である。

通信端末150は、CPU151、ROM152、RAM153、HDD154、通信I/F155、入力装置（入力手段）156、表示装置（表示手段）157を備え、これらがシステムバス158によって接続されている。

図13は、工場端末160のハードウェア構成例を示すブロック図である。

工場端末160は、CPU161、ROM162、RAM163、通信I/F164を備え、これらがシステムバス166によって接続されている。

【0075】

通信端末150および工場端末160によれば、CPU151がROM152やHDD154に記憶されている各種制御プログラムを実行することによって通信端末150の動作を、CPU161がROM132やHDD134に記憶されている各種制御プログラムを実行することによって工場端末160の動作をそれぞれ制御し、この発明による機能（デジタル証明書送信要求手段、デジタル証明書送信手段、デジタル証明書保存手段、書き込み済み情報設定手段、デジタル証明書削除手段としての機能等）を実現することができる。

なお、証明書管理装置607、通信端末150、工場端末160のハードウェアとしては、適宜公知のコンピュータを採用することができる。もちろん、必要に応じて他のハードウェアを付加してもよい。

【0076】

図14は、生産工場Eにおける通信端末150および工場端末160の周辺を示すブロック図である。

通信端末150は、セキュリティ面を考慮し、生産工場Eの管理者室Fに設置されている。その管理者室Fは、特定の管理者しか入れないように、ドアGに鍵をかけるようにしている。また、通信端末150は、特定のID、パスワードが入力された場合にのみ、操作できるようにしている。

この例では、生産工場Eには、仲介装置101の生産用ライン1001、画像形成装置100の生産用ライン1002、画像形成装置110の生産用ライン1003がある。そして、その各生産用ライン1001、1002、1003毎に工場端末160（160a、160b、160c）が設置されている。

【0077】

各工場端末160にはそれぞれ、バーコードリーダ141（141a, 141b, 141c）と接続するためのバーコード用I/F142（142a, 142b, 142c）、および通信装置（仲介装置101, 画像形成装置100, 110）と接続するための書き込み用I/F165（165a, 165b, 165c）がそれぞれ接続されている。

図15は、工場端末160とバーコードリーダ141と通信装置との接続例を示す図である。

【0078】

この図15を見て分かるように、工場端末160bに、バーコード用I/F142bを介してバーコードリーダ141bが、書き込み用I/F165を介して画像形成装置100がそれぞれ接続されている。

なお、画像形成装置100（又は画像形成装置110や仲介装置101）は、初期値として同じIPアドレスを有しており、工場端末160とLAN接続すると、IPアドレスが重複してしまうため、クロスケーブル（書き込み用I/F165を使用して工場端末160と接続している。

図16は、画像形成装置100又は110に貼付された定格銘板の一例を示す図である。

この定格銘板の機種機番を示すバーコードBCの情報を、バーコードリーダ141によって読み取ることができる。

【0079】

図17は、図14に示した生産工場Eの各生産用ライン1001, 1002, 1003での通信装置の生産工程の一例を示す説明図である。

各生産用ライン1001, 1002, 1003ではそれぞれ、まず通信装置（仲介装置101, 画像形成装置100, 110）の制御基板が組み立てられ、次にその制御基板の検査が行われた後、工場端末160によって固定値を共通証明書としてフラッシュメモリ204およびNVRAM207に書き込まれる。

その後、フラッシュメモリ204およびNVRAM207に共通証明書が書き込まれた制御基板が梱包され、サービス部品として出荷される。

【0080】

あるいは、フラッシュメモリ 204 および NVRAM 207 に共通証明書が書き込まれた制御基板は、製品用として次工程へ送られる。そして、その制御基板は予め組み立てられた画像形成装置 100 又は 110 のカバーに合わせられ、その画像形成装置 100 又は 110 に搭載され、製品が出来あがる。

その製品となった画像形成装置 100 又は 110 は、その機能検査が行われた後、通信端末 150 および工場端末 160 によって証明書がフラッシュメモリ 204 に書き込まれると共に、フラッシュメモリ 204 内のパラメータが初期化される。

その後、その画像形成装置 100 又は 110 は、外観が検査された後、梱包され、出荷される。

なお、制御基板の組み立てと製品の組み立ては、別工場で行うことが多い。

【0081】

次に、上述した画像形成装置管理システム（情報管理システム）における実施形態、つまりこの発明の特徴となる動作（証明書取得処理）について、図 18 ～ 図 23 を参照して具体的に説明する。

図 18 は、この画像形成装置遠隔管理システムにおける証明書取得処理時の通信シーケンスの一例を示す図である。

図 19 は、通信端末 150 の HDD 154 内の工場製造管理 DB の一例を示す図である。

図 19 の（a）は証明書管理機器一覧 DB の一例を示しており、機種コード別の証明書の有無を示している。同図の（b）は生産計画 DB の一例を示しており、機種コード別の日々の生産台数を示している。

【0082】

図 20 は、通信端末装置 150 の HDD 154 内の証明書 DB 154 a の一例を示す図である。

証明書 DB 154 a は、機種機番別の証明書、その作成日、その書き込み済みフラグの状態を示している。そのうち、証明書（デジタル証明書）は、ルート証明書（ルート鍵証明書）、クライアント証明書（クライアント公開鍵証明書）、

秘密鍵（クライアント私有鍵）のバックになっている。

図 21 は、証明書管理装置 607 と通信端末 150 との通信時のデータフォーマットの一例を示す図である。

図 22 は、通信端末 150 と工場端末 160 との通信時のデータフォーマットの一例を示す図である。

図 23 は、工場端末 160 と通信装置（画像形成装置 100 等）との通信時のデータフォーマットの一例を示す図である。

【0083】

通信端末 150 の CPU 151 は、毎月、所定のタイミングで（予め決められた日時に）生産管理システム 140 から各通信装置（画像形成装置 100 等）の日々の生産台数を取得し、HDD 154 内の生産計画 DB に保存することにより、その生産計画 DB を更新する。

を更新する。また、毎日、所定のタイミングで（予め決められた時刻）に、HDD 154 内の証明書管理機器一覧 DB および生産計画 DB に基づいて、本日生産（製造）された各通信装置による通信時の SSL による相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）を本日の生産台数分だけ付加して証明書管理装置 607 へ通知する。なお、1 台の通信装置毎に通信要求を通知することもできる。

【0084】

証明書管理装置 607 の CPU 131 は、通信端末 150 から証明書の送信要求を受けた場合に、その送信要求に付加された機種機番を含む証明書をその機種機番数だけ生成し、その各証明書を通信端末 150 へ送信する。

なお、通信端末 150 と証明書管理装置 607 とは、共通証明書を用いて SSL による相互認証を行った後、図 21 に示すような SOAP（構造化言語形式である XML 形式）によるデータフォーマットで SSL 通信を行うようにしている。

通信端末 150 の CPU 151 は、証明書管理装置 607 への各機種機番を含む証明書の送信要求に対して、その証明書管理装置 607 からその各機種機番をそれぞれ含む各証明書を受信すると、それらの証明書を HDD 154 内の証明書

DB154aに保存することにより、その証明書DBを更新する。

【0085】

工場端末160のCPU161は、本日生産された各通信装置に貼付された定格銘板あるいは対応するチェックシートから機種機番を示すバーコードがバーコードリーダ141によって順次読み取られ、その各バーコードによる機種機番が順次入力されると、その入力順に、そのバーコードによる機種機番を含む証明書の送信要求を通信端末150へ通知する。

通信端末150のCPU151は、工場端末160からバーコードによる機種機番を含む証明書の送信要求を受けた場合に、その機種機番に対応する証明書をHDD154内の証明書DBから読み出して工場端末160へ送信する。

工場端末160のCPU161は、通信端末150への機種機番を含む証明書の送信要求に対して、その通信端末150から証明書を受信すると、その証明書を該当する通信装置（機種機番が読み取られた通信装置）へ送信する。

【0086】

通信装置のCPUは、工場端末160から証明書を受信すると、受信応答を工場端末160へ通知した後、その証明書を内部の不揮発性メモリ（画像形成装置100の場合はフラッシュメモリ204）に書き込み、その書き込みが正常に終了したことを確認できた場合には、証明書の書き込みが完了（成功）した旨を示す書き込み結果を工場端末160へ通知する。証明書の書き込みが正常に終了しなかったことを確認できた場合には、証明書の書き込みが失敗した旨を示す書き込み結果を工場端末160へ通知する。

工場端末160のCPU161は、該当する通信装置への証明書の送信に対して、その通信装置から受信応答の通知を受けると、その受信応答を通信端末150へ通知する。続いて、書き込み結果の通知を受けると、その書き込み結果を通信端末150へ通知する。

【0087】

通信端末150のCPU151は、工場端末160への証明書の送信に対して、工場端末160から受信応答の通知に続いて書き込み結果の通知を受けると、受信応答を工場端末160へ通知した後、その書き込み結果から証明書の書き込

みが完了したことを確認できた場合には、証明書DB154a（図20）における対応する証明書（書き込みが完了した証明書）の書き込み済みを示す書き込み済みフラグ（情報）を“1”（済み）にセット（設定）する。証明書の書き込みが失敗したことを確認できた場合には、対応する機種機番を含む証明書の送信要求を証明書管理装置607へ通知することにより、上述と同様にして新たな証明書を取得した後、その証明書を通信端末150へ通知し、以後上述と同様の処理を行う。

【0088】

なお、証明書DB154aに、同じ証明書を長く保持すると、セキュリティの問題もあるため、工場端末160から書き込み結果の通知を受けた場合に、対応する証明書を証明書DB154aから削除するようにしてもよい。

工場端末160のCPU161は、通信端末150への受信応答および書き込み結果の通知に対して、その通信端末150から受信応答の通知を受けると、その受信応答を該当する通信装置へ通知する。

【0089】

なお、通信端末150と工場端末160とは、図22に示すようなSOAPによるデータフォーマットで通信を行うようにしている。

また、工場端末160と該当する通信装置とは、共通証明書を用いてSSLによる相互認証を行った後、図23に示すようなSOAPによるデータフォーマットでSSL通信を行うようにしている。この場合、工場端末160のCPU161は該当する通信装置へ送信すべき証明書を暗号化し、その通信装置のCPUは工場端末160から受信した暗号化された証明書をそのまま不揮発性メモリに書き込むか、復号化した後不揮発性メモリに書き込むようにしている。

【0090】

さらに、この実施形態では、各通信装置の機種機番をバーコードリーダによって読み取って工場端末160へ入力するようにしているが、例えば信端末150の入力装置156を操作することにより、各通信装置の機種機番を入力するようにしてもよい。

さらにまた、ある機種の生産が打ち切られた場合には、計画的に処理を行うが

、何らかの事情で通信端末150の証明書DB154aに対応する証明書（生産が打ち切りとなった通信装置の機種に対応する証明書）が残ったままになっていた場合には、管理責任者が通信端末150の入力装置156を操作することにより、対応する証明書を証明書DB154aから削除（消去）することもできる。

また、通信端末150のCPU151は、現在有している機種毎の証明書の数と当日使用した証明書の数を表示装置157に表示させることもできる。

【0091】

この実施形態においては、以下の（１）～（５）に示す作用効果を得ることができる。

（１）通信端末150のCPU151が、生産されたある通信装置によるSSL通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）をその通信装置の生産台数分だけ付加して証明書管理装置607へ通知し、その各機種機番を付加した証明書の要求通知に対して、その証明書管理装置607からその各機種機番をそれぞれ含む各証明書を受信した場合に、その各証明書を証明書DB154aに保存した後、上記生産台数分の通信装置のいずれかに貼付された定格銘板あるいは対応するチェックシート上の機種機番を示すバーコードがバーコードリーダ141によって読み取られ、そのバーコードによる機種機番が工場端末160経由で入力された場合に、その機種機番に対応する証明書を証明書DB154aから読み出して工場端末160によって上記ある通信装置（機種機番が読み取られた通信装置）へ送信させ、その通信装置の不揮発性メモリに書き込ませる。

それによって、中央管理装置102側が、その通信装置とSSL通信する際の相互認証時に、その通信装置から受信した証明書内の機種機番をチェックすることにより、その通信装置が保守契約したものであるかどうかを正確に判定することが可能になる。

【0092】

（２）通信端末150のCPU151が、生産されたある通信装置によるSSL通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）をその通信装置の生産台数分だけ付加して証明書管理装置607へ通知し、

その各機種機番を付加した証明書の要求通知に対して、その証明書管理装置 607 からその各機種機番をそれぞれ含む各証明書を受信した場合に、その各証明書を証明書 DB 154 a に保存した後、上記生産台数分の通信装置のいずれかが入力装置 156 によって入力された場合に、その機種機番に対応する証明書を証明書 DB 154 a から読み出して工場端末 160 によって上記ある通信装置へ送信させ、その通信装置の不揮発性メモリに書き込ませる。

それによって、(1) と同様の効果を得ることができる。但し、入力装置 156 の操作によって機種機番を入力するため、入力ミスしないように注意する必要がある。

【0093】

(3) (1) 又は (2) の工場端末 160 から対応する通信装置への証明書の送信の際に、工場端末 160 の CPU 161 が、その通信装置との間で共通証明書を用いて相互認証を行い、その通信装置へ送信すべき証明書を暗号化する。

それによって、工場端末 160 と通信装置との間の通信のセキュリティが向上する。

(4) 通信端末 150 の CPU 151 が、対応する通信装置の不揮発性メモリへの証明書の書き込みが完了した場合に、証明書 DB 154 a におけるその証明書の書き込み済みを示す書き込み済みフラグを“1”にセットする。

それによって、証明書の書き込みが完了した通信装置を特定することができるため、通信装置の生産性の向上につながる。

【0094】

(5) 通信端末 150 の CPU 151 が、対応する通信装置の不揮発性メモリへの証明書の書き込みが完了した場合に、その証明書を証明書 DB 154 a から削除する。

それによって、(4) と同様の効果を得られる。また、証明書 DB 154 a に、同じ証明書を長く保持すると、セキュリティの問題もあるため、書き込みが完了した証明書を証明書 DB 154 a から削除すれば、セキュリティの向上につながる。

【0095】

なお、通信端末150のCPU151が、生産されたある通信装置によるSSL通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番（識別情報）を付加して証明書管理装置607へ通知し、その機種機番を付加した証明書の要求通知に対して、その証明書管理装置607からその機種機番を含む証明書を受信した場合に、その証明書を工場端末160によって上記ある通信装置へ送信させ、その通信装置の不揮発性メモリに書き込ませることもできる。このようにすれば、証明書DB154aをなくすこともでき、低コストにつながる。

【0096】

以上、この発明を画像形成装置100、110、および仲介装置101の不揮発性メモリに証明書を書き込むための通信端末150および工場端末160に適用した実施形態について説明したが、この発明はこれに限らず、ネットワーク家電、自動販売機、医療機器、電源装置、空調システム、ガス・水道・電気等の計量システム等や、ネットワークに接続可能なコンピュータ等の通信装置の不揮発性メモリに証明書を書き込むための情報処理装置に適用可能である。

また、この発明によるプログラムは、通信端末150および工場端末160を制御するコンピュータ（CPU131、151）に、この発明による各機能（デジタル証明書生成手段、デジタル証明書送信手段、書き込み済み情報設定手段、デジタル証明書削除手段としての機能等）を実現させるためのプログラムであり、このようなプログラムをコンピュータに実行させることにより、上述したような効果を得ることができる。

【0097】

このようなプログラムは、はじめからコンピュータに備えるROMあるいはHDD等の記憶手段に格納しておいてもよいが、記録媒体であるCD-ROMあるいはフレキシブルディスク、SRAM、EEPROM、メモリカード等の不揮発性記録媒体（メモリ）に記録して提供することもできる。そのメモリに記録されたプログラムをコンピュータにインストールしてCPUに実行させるか、CPUにそのメモリからこのプログラムを読み出して実行させることにより、上述した各手順を実行させることができる。

さらに、ネットワークに接続され、プログラムを記録した記録媒体を備える外

部機器あるいはプログラムを記憶手段に記憶した外部機器からダウンロードして実行させることも可能である。

【0098】

【発明の効果】

以上説明してきたように、この発明によれば、中央管理装置側が、通信装置と通信する際の認証時に、その通信装置が保守契約したものであるかどうかを正確に判定することができる。

【図面の簡単な説明】

【図1】

この発明による通信装置を被管理装置とする遠隔管理システムの構成例を示す概念図である。

【図2】

その遠隔管理システムにおけるデータ送受モデルを示す概念図である。

【図3】

この発明による電子装置を画像形成装置とする画像形成装置遠隔管理システムの構成例を示す概念図である。

【図4】

図3の画像形成装置100のハードウェア構成例を示すブロック図である。

【図5】

図4のフラッシュメモリ204の記憶エリアの構成例を示すメモリマップ図である。

【図6】

図4のNVRAM207の記憶エリアの構成例を示すメモリマップ図である。

【図7】

図3の画像形成装置100（又は110）のソフトウェア構成例を示すブロック図である。

【図8】

図7のNRS305の構成例を示す機能ブロック図である。

【図9】

図 3 の中央管理装置 1 0 2 の概略構成例を示すブロック図である。

【図 1 0】

図 3 の生産工場 E の内部構成例を示すブロック図である。

【図 1 1】

図 1 0 の証明書管理装置 6 0 7 のハードウェア構成例を示すブロック図である。

【図 1 2】

図 1 0 の通信端末 1 5 0 のハードウェア構成例を示すブロック図である。

【図 1 3】

図 1 0 の工場端末 1 6 0 のハードウェア構成例を示すブロック図である。

【図 1 4】

図 1 0 の生産工場 E における通信端末 1 5 0 および工場端末 1 6 0 の周辺を示すブロック図である。

【図 1 5】

図 1 0 の工場端末 1 6 0 とバーコードリーダー 1 4 1 と通信装置との接続例を示す図である。

【図 1 6】

図 1 0 の画像形成装置 1 0 0 又は 1 1 0 に貼付された定格銘板の一例を示す図である。

【図 1 7】

図 1 4 に示した生産工場 E の各生産用ライン 1 0 0 1, 1 0 0 2, 1 0 0 3 での通信装置の生産工程の一例を示す説明図である。

【図 1 8】

図 1 0 の生産工場 E 内の通信端末 1 5 0 および工場端末 1 6 0 による証明書取得処理時の通信シーケンスの一例を示す図である。

【図 1 9】

図 1 2 の HDD 1 5 4 内の工場製造管理 DB の一例を示す図である。

【図 2 0】

図 1 2 の HDD 1 5 4 内の証明書 DB の一例を示す図である。

【図 2 1】

図 1 0 の証明書管理装置 6 0 7 と通信端末 1 5 0 との通信時のデータフォーマットの一例を示す図である。

【図 2 2】

図 1 0 の通信端末 1 5 0 と工場端末 1 6 0 との通信時のデータフォーマットの一例を示す図である。

【図 2 3】

図 1 0 の工場端末 1 6 0 と通信装置（画像形成装置 1 0 0 等）との通信時のデータフォーマットの一例を示す図である。

【図 2 4】

クライアント装置とサーバ装置とが S S L による相互認証を行う際の各装置において実行する処理のフローチャートを、その処理に用いる情報と共に示す図である。

【図 2 5】

図 2 4 に示した認証処理におけるルート鍵、ルート私有鍵、およびクライアント公開鍵の関係について説明するための図である。

【符号の説明】

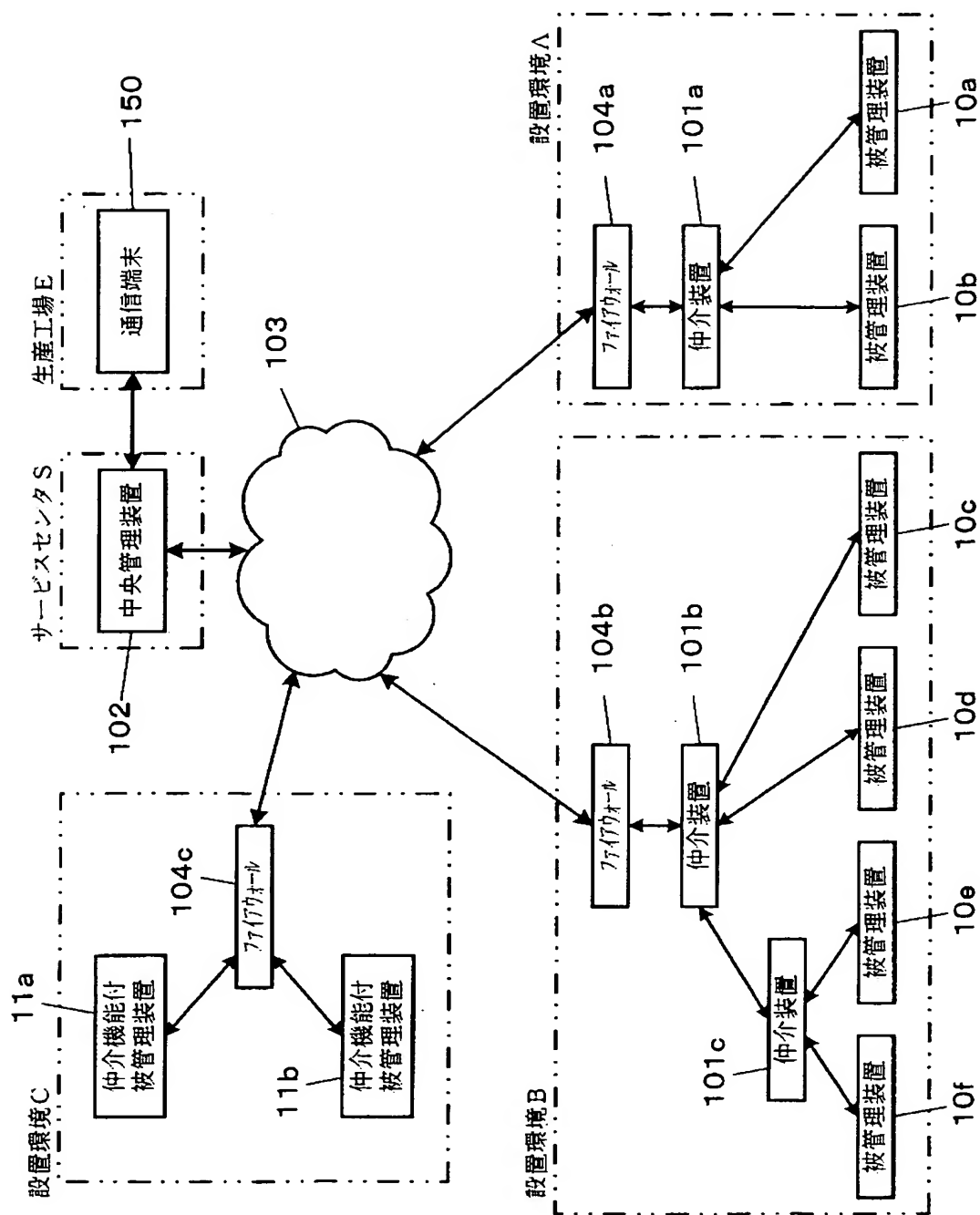
1 0 : 被管理装置	1 1 : 仲介機能付被管理装置
1 0 0 : 画像形成装置	1 0 1 : 仲介装置
1 0 2 : 管理装置	1 0 3 : インタネット
1 0 4 : ファイアウォール	
1 1 0 : 仲介機能付画像形成装置	
1 3 1, 1 5 1, 1 6 1, 2 0 1 : CPU	
1 3 2, 1 5 2, 1 6 2 : ROM	
1 3 3, 1 5 3, 1 6 3 : RAM	
1 3 4, 1 5 4, 2 1 0 : HDD	
1 3 5, 1 5 5, 1 6 4 : 通信 I / F	
1 5 6 : 入力装置	1 5 7 : 表示装置
1 4 0 : 生産管理システム	1 4 1 : バーコードリーダー

1 5 0, 6 0 2 : 通信端末 1 6 0 : 工場端末
2 0 2 : A S I C 2 0 3 : S D R A M
2 0 4 : フラッシュメモリ 2 0 5 : N R S 用メモリ
2 0 6 : P H Y 2 0 7 : N V R A M
2 0 9 : 操作部 2 1 2 : P I
3 0 0 : O C S 3 0 1 : E C S
3 0 2 : M C S 3 0 3 : N C S
3 0 4 : F C S 3 0 5 : N R S
3 0 6 : S C S 3 0 7 : S R M
3 0 8 : I M H 3 0 9 : コピーアプリ
3 1 0 : ファクスアプリ 3 1 1 : プリンタアプリ
3 1 2 : スキャナアプリ
3 1 3 : ネットファイルアプリ 3 1 4 : ウェブアプリ
6 0 1 : モデム
6 0 3 : プロキシサーバ 6 0 4 : 操作者端末
6 0 5 : 外部接続 I / F 6 0 6 : ファイルサーバ
6 0 7 : 証明書管理装置 6 0 8 : 制御装置

【書類名】

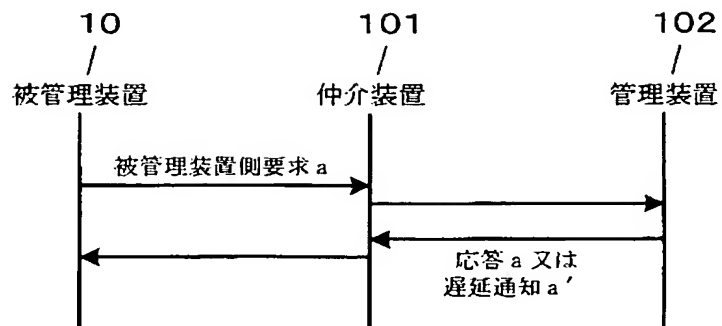
図面

【図 1】

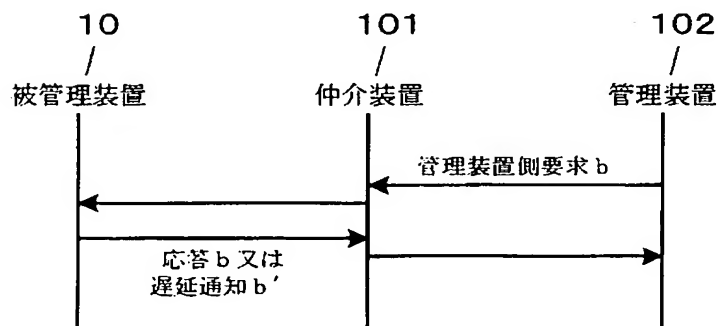


【図 2】

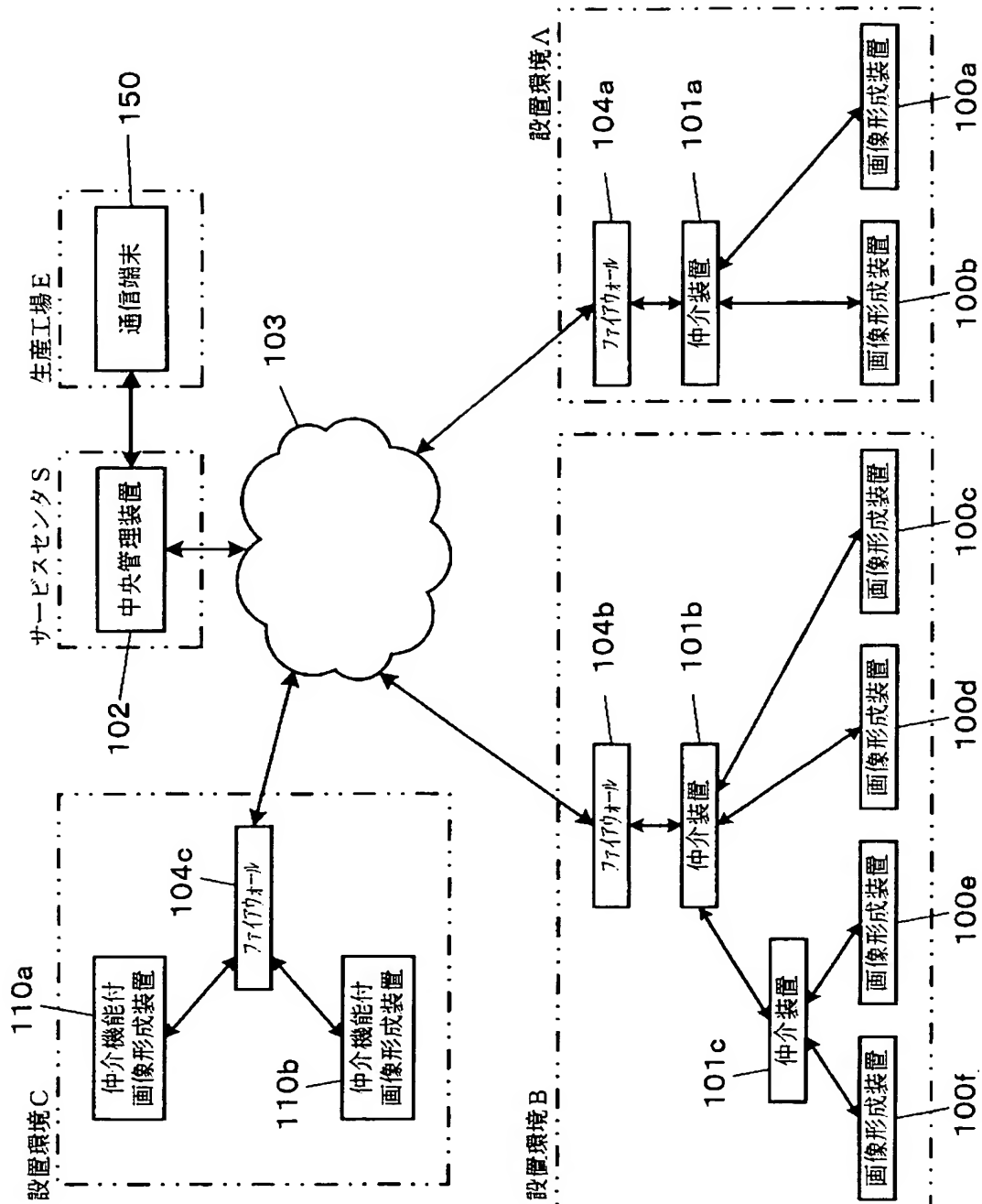
(A)



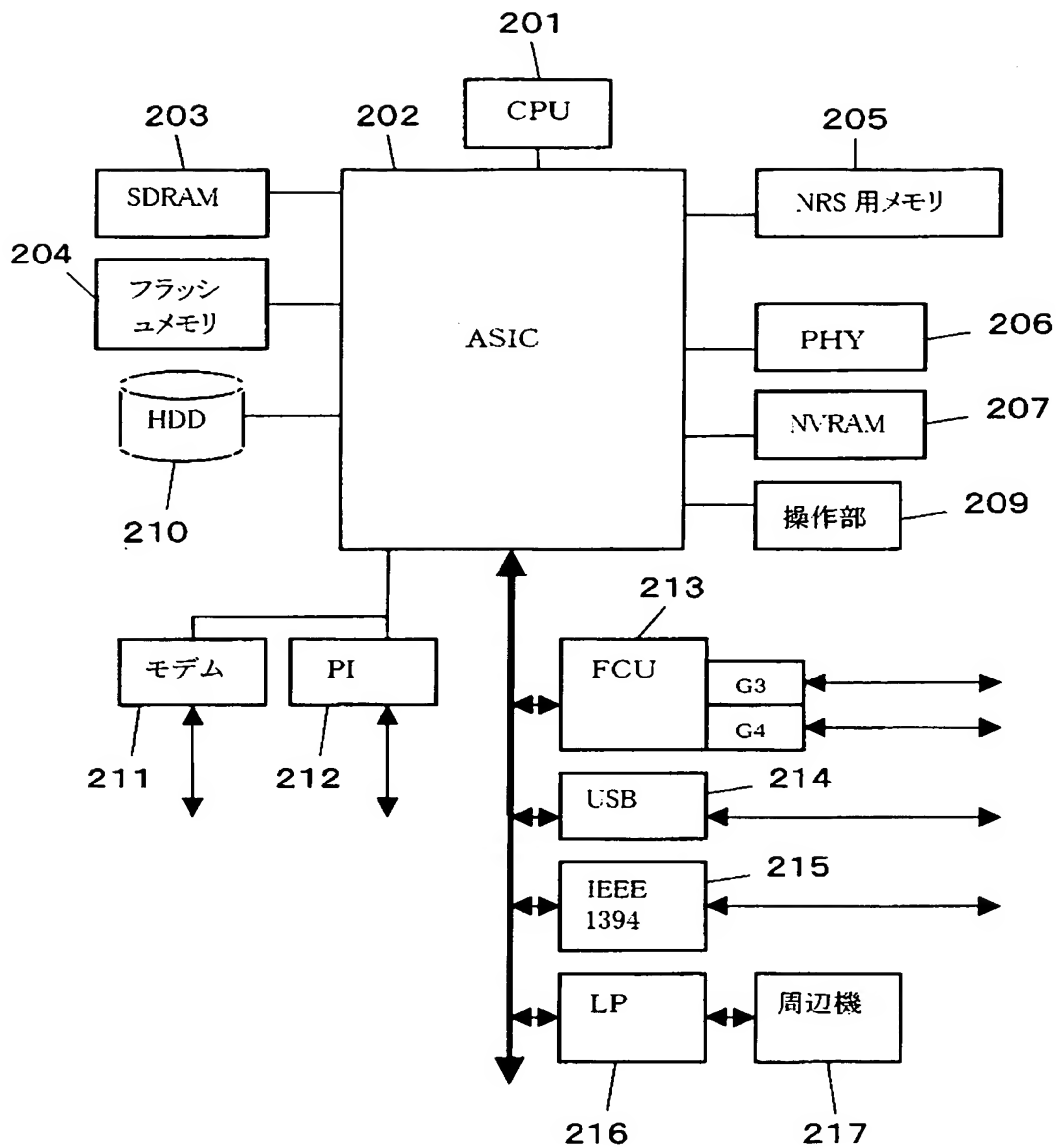
(B)



【図 3】



【図 4】



【図 5】

フラッシュメモリ

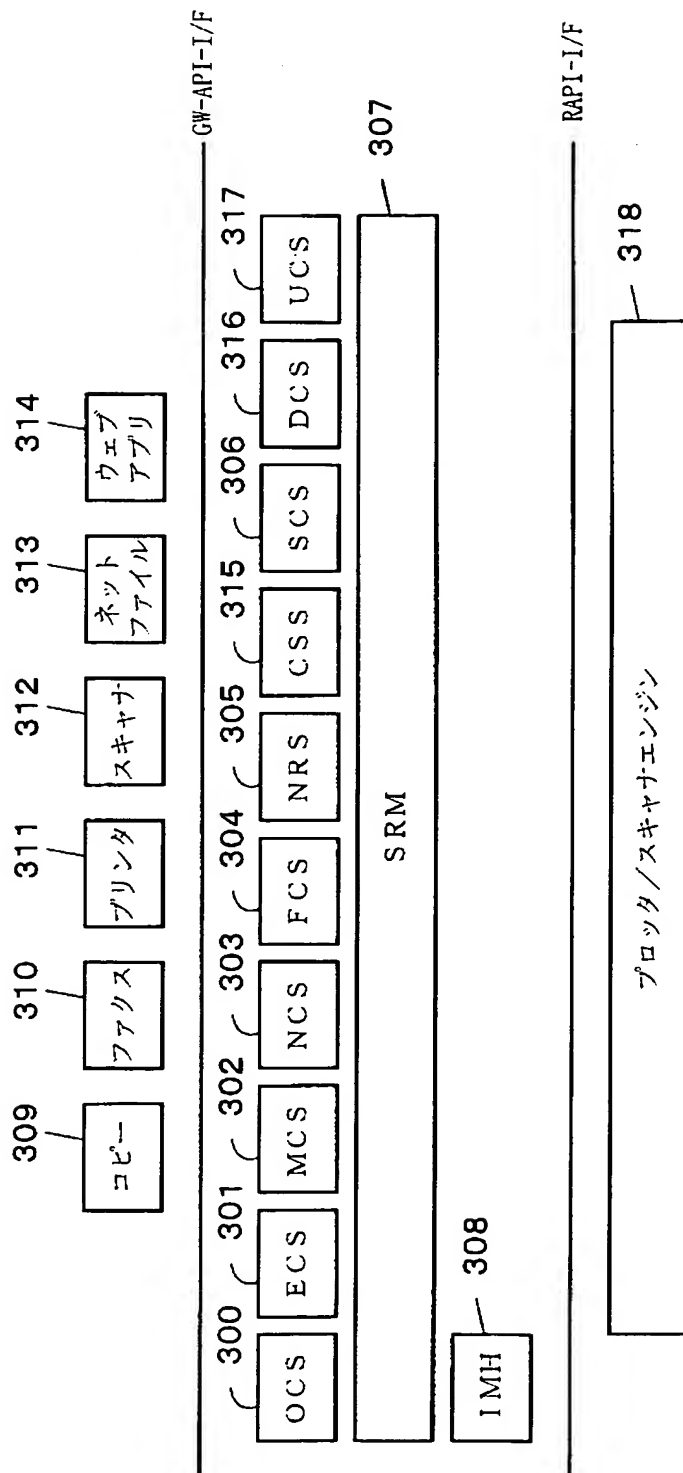
証明書
共通証明書
固定パラメータエリア
プログラムエリア

【図 6】

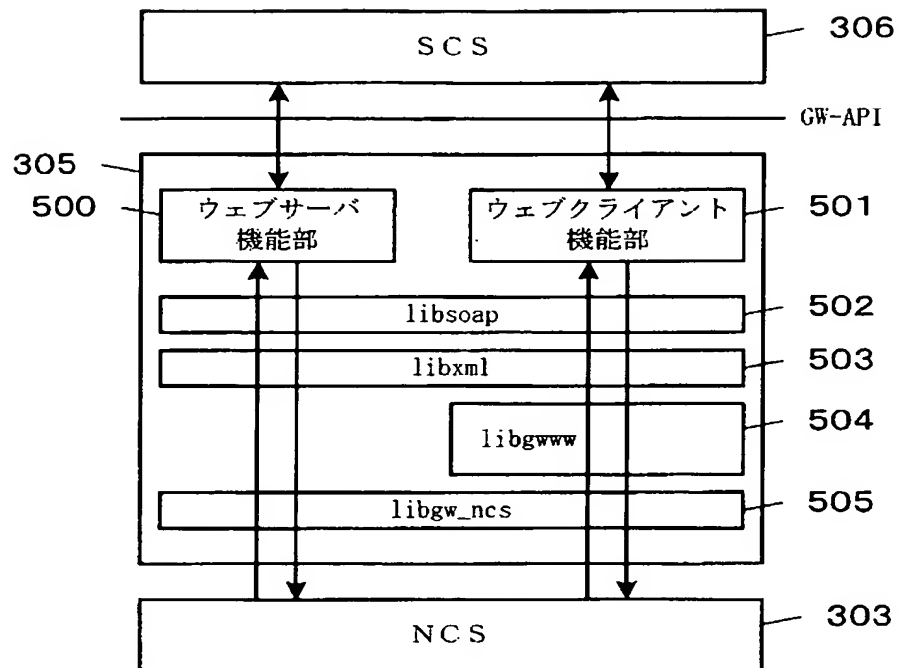
NVRAM

機種機番
操作上の初期値
各APLの初期値
各カウンタ情報
共通証明書

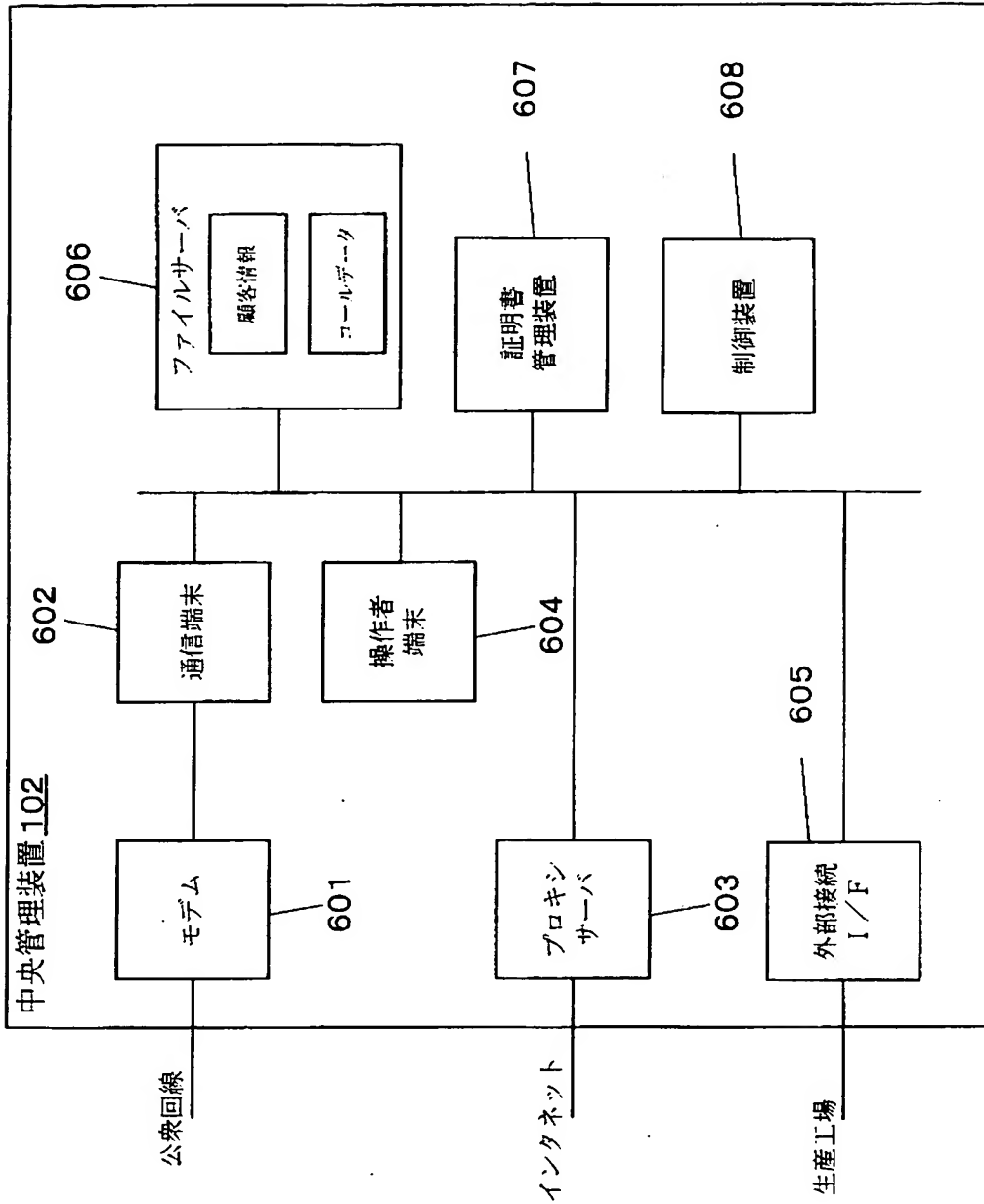
【図 7】



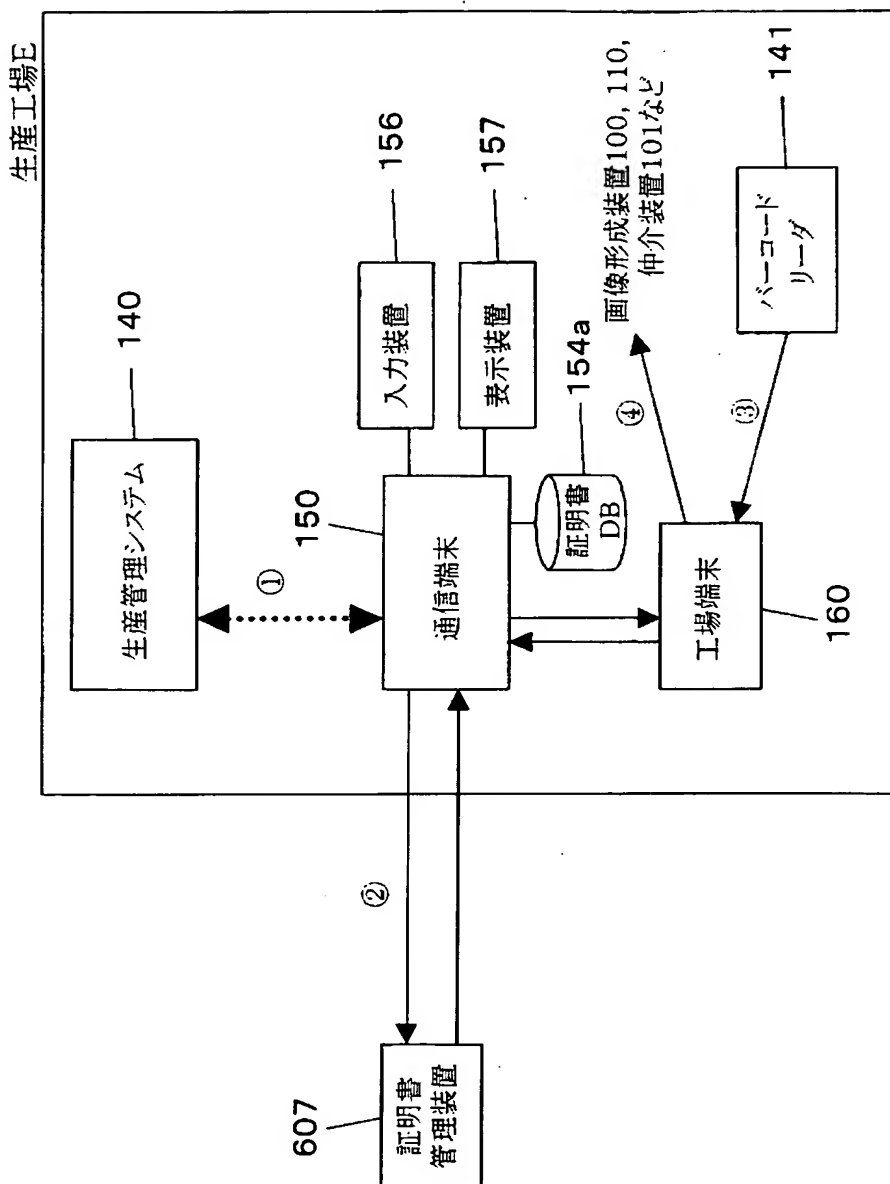
【図 8】



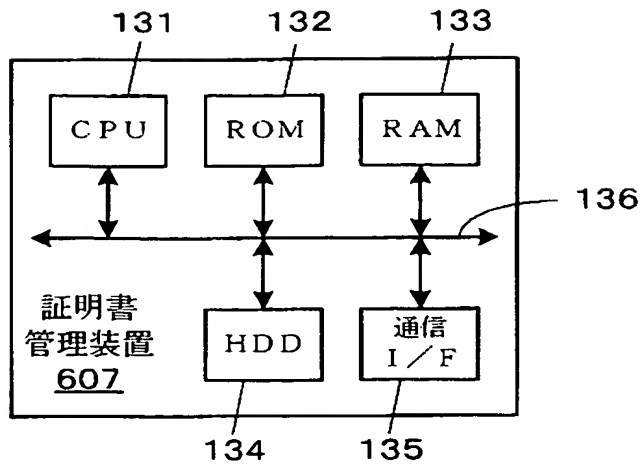
【図 9】



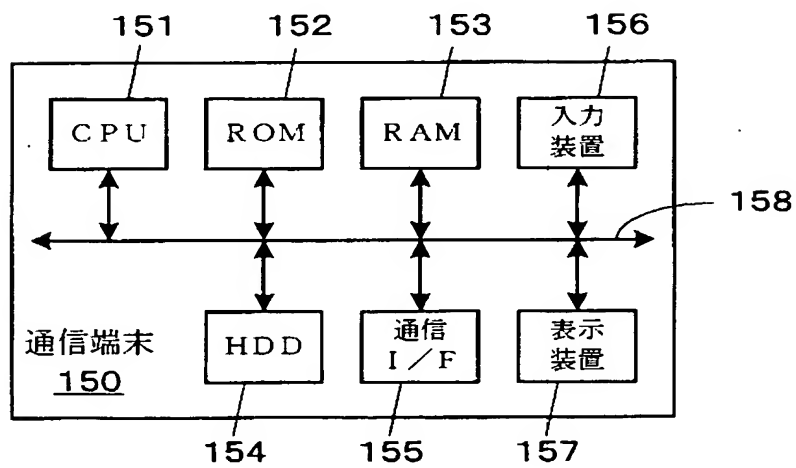
【図 10】



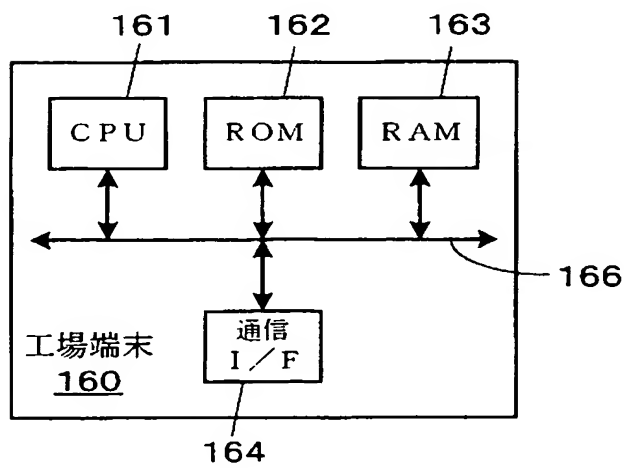
【図 1 1】



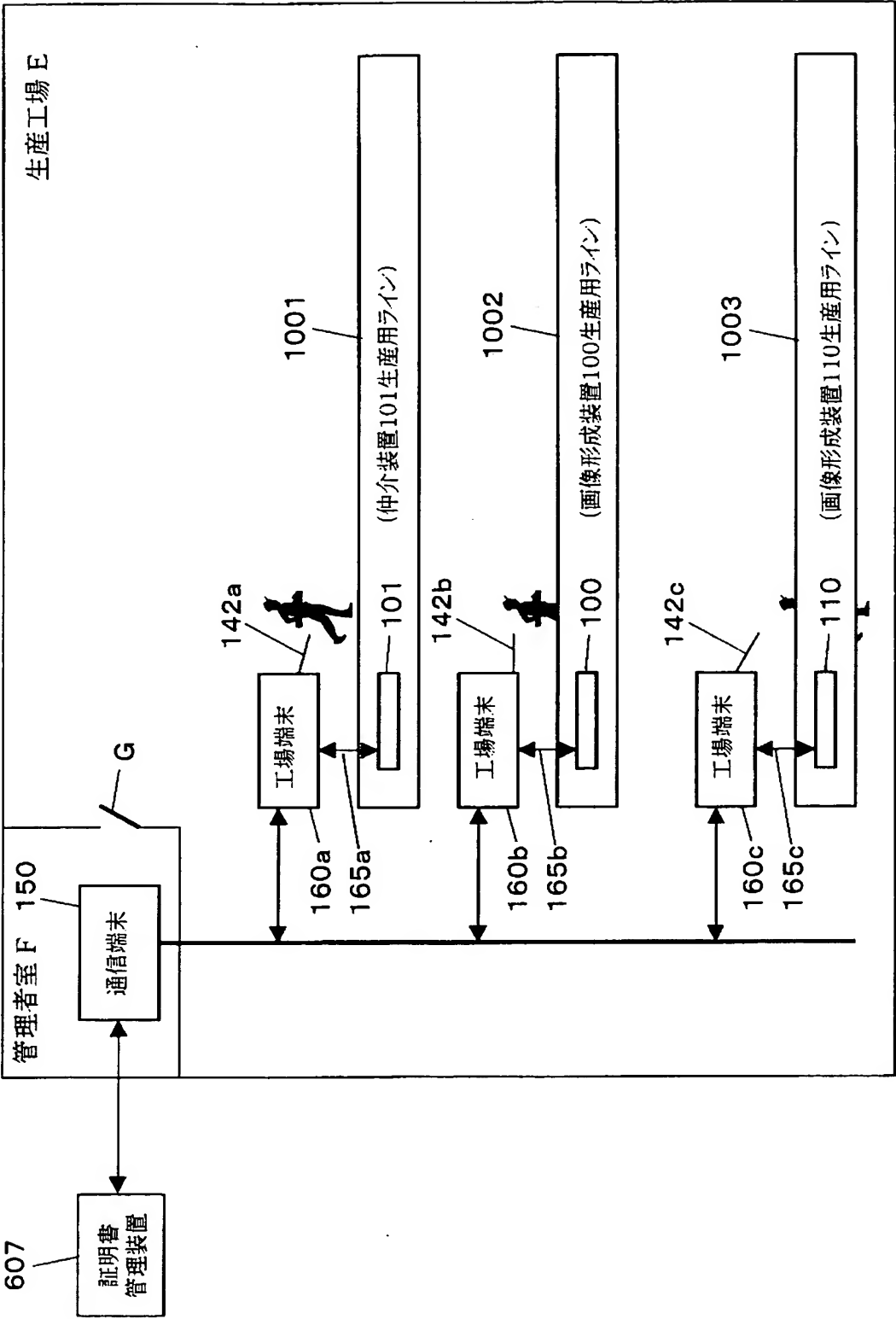
【図 1 2】



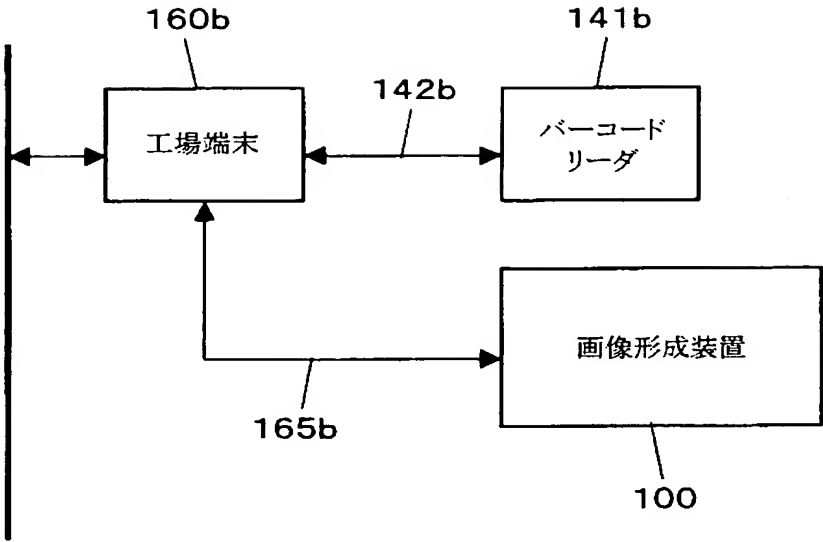
【図 1 3】



【図 14】



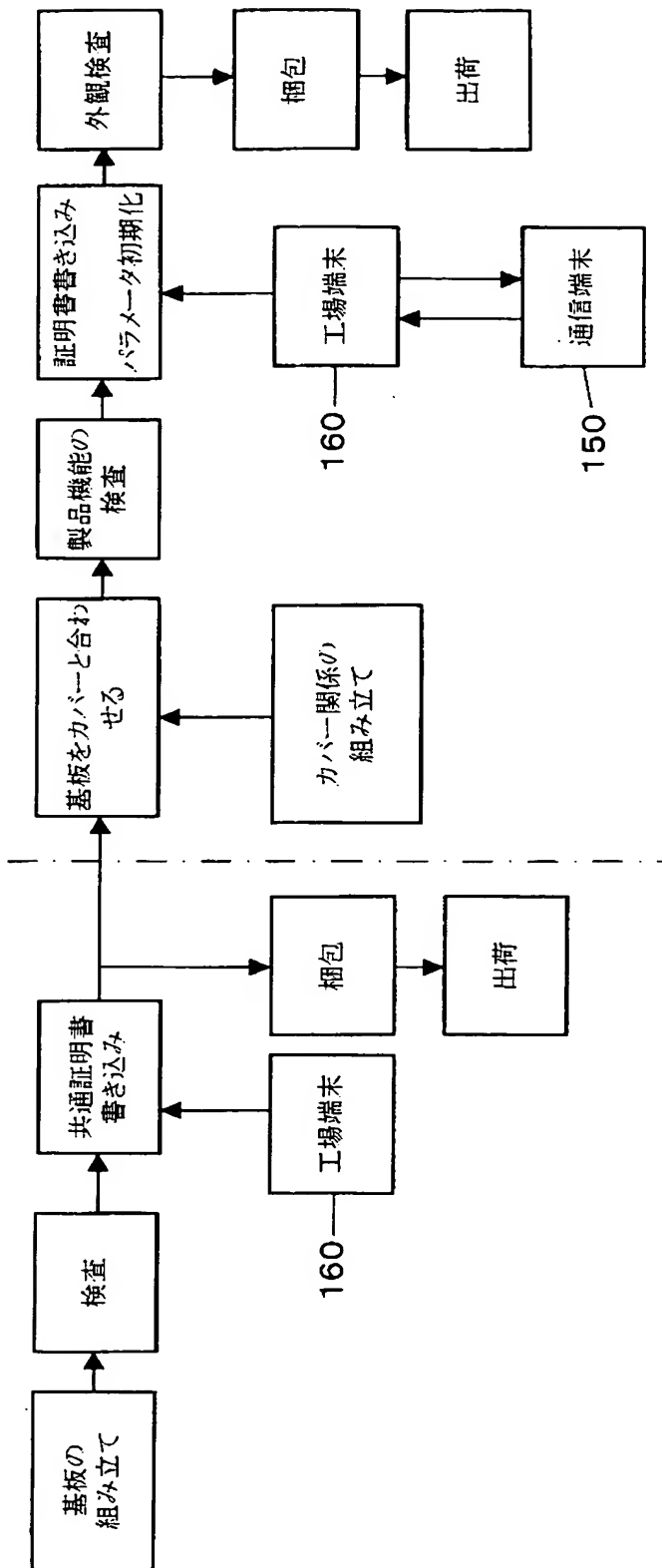
【図 15】



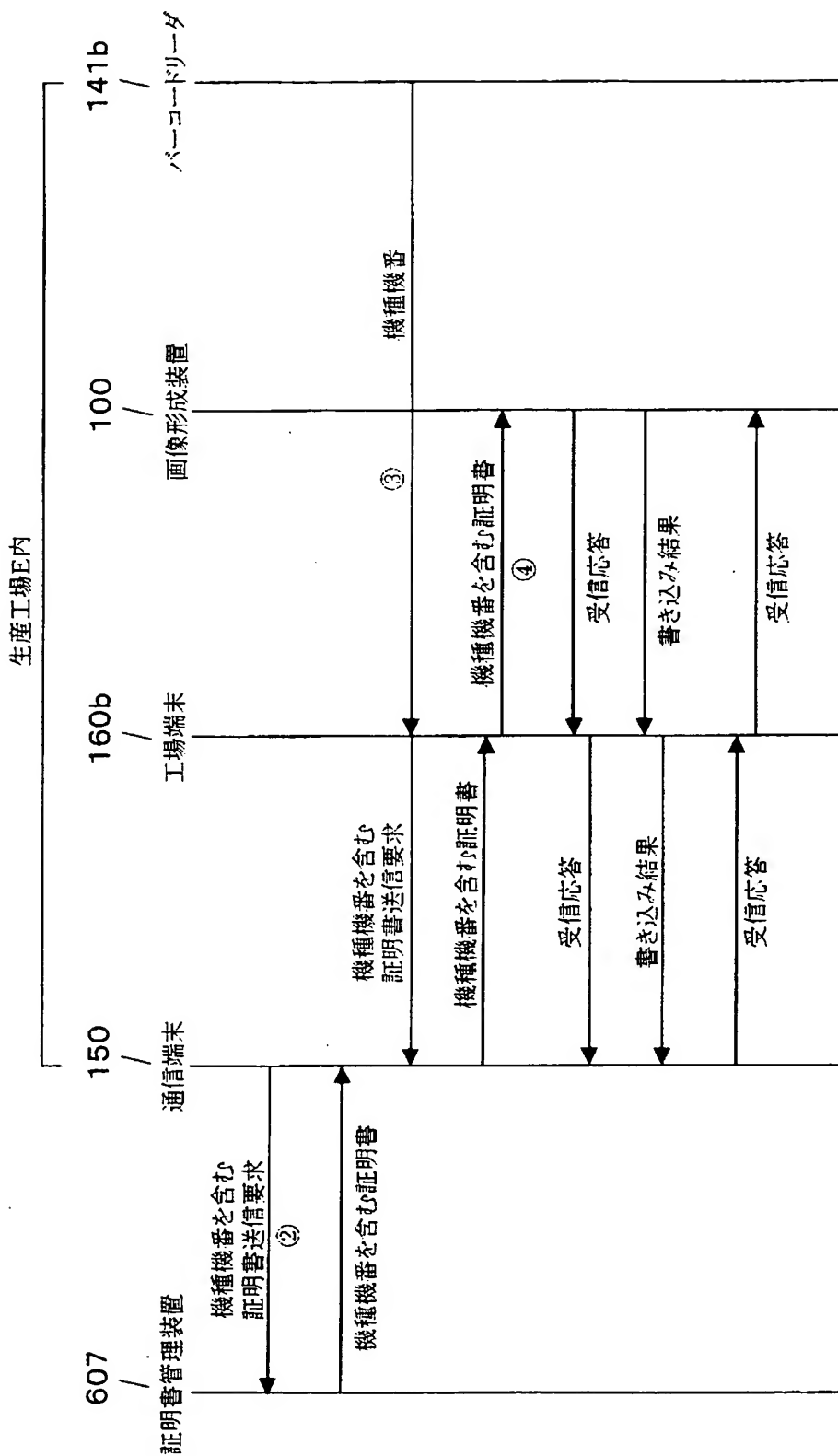
【図 16】

AICOO 画像形成装置 TYPE-1			
定格電圧	定格消費電力	定格電流	機種コード
DC12V	3VA	0.25A	H100-00
機種機番	バーコード BC		

【図 17】



【図 18】



【図 1 9】

No	機種コード	証明書の有無	備考
1	3012	有り	
2	3013	なし	
3	3014	なし	
4	A123	有り	
5	A125	なし	

(a)

機種コード	3/17	3/18	3/19	3/20	3/24	3/25	3/26	3/27
3012	1000	1010	1020	1000	900	1200	1300	1100
3013	500	550	500	560	530	550	530	530
3014	560	570	560	560	540	570	550	550
A123	2120	2000	2130	2000	2000	2130	2110	2000
A125	2000	2001	2010	2020	2010	2000	2300	2000

(b)

【図 2 0】

機種機番	証明書	作成日	書込み済 Flag
3012-123456	証明書 1 パック	20030308	済み
3012-123457	証明書 2 パック	20030308	済み
3012-123458	証明書 3 パック	20030308	
3012-123459	証明書 4 パック	20030308	
A123-654321	証明書 5 パック	20030308	
A123-654322	証明書 6 パック	20030308	

ルート証明書 - 1	クライアント証明書 (A123-654322)	秘密鍵 (A123-654322)
------------	-------------------------	-------------------

【図 2 1】

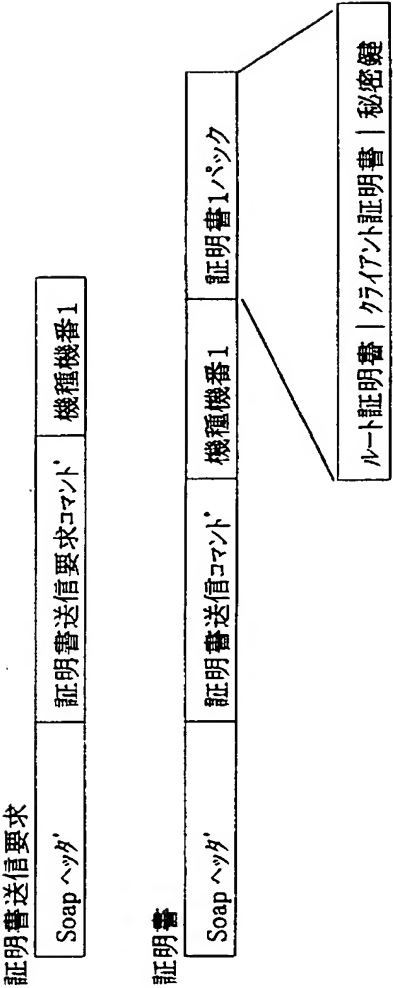
証明書送信要求

Soap ヘッダ	証明書送信要求コメント	機種機番 1, 機種機番 2, 機種機番 3, ……機種機番 n
----------	-------------	----------------------------------

証明書

Soap ヘッダ	証明書送信コメント	機種機番 1 証明書 1 パック, 機種機番 2 証明書 2 パック, 機種機番 3 証明書 3 パック, ; 機種機番 n 証明書 n パック
----------	-----------	--

【図 2 2】



【図 2 3】

証明書

Soap ヘッダ'	証明書送信コマンド'	証明書1パック
-----------	------------	---------

(a)

受信応答

Soap ヘッダ'	証明書受信応答コマンド'	OK
-----------	--------------	----

書き込み結果

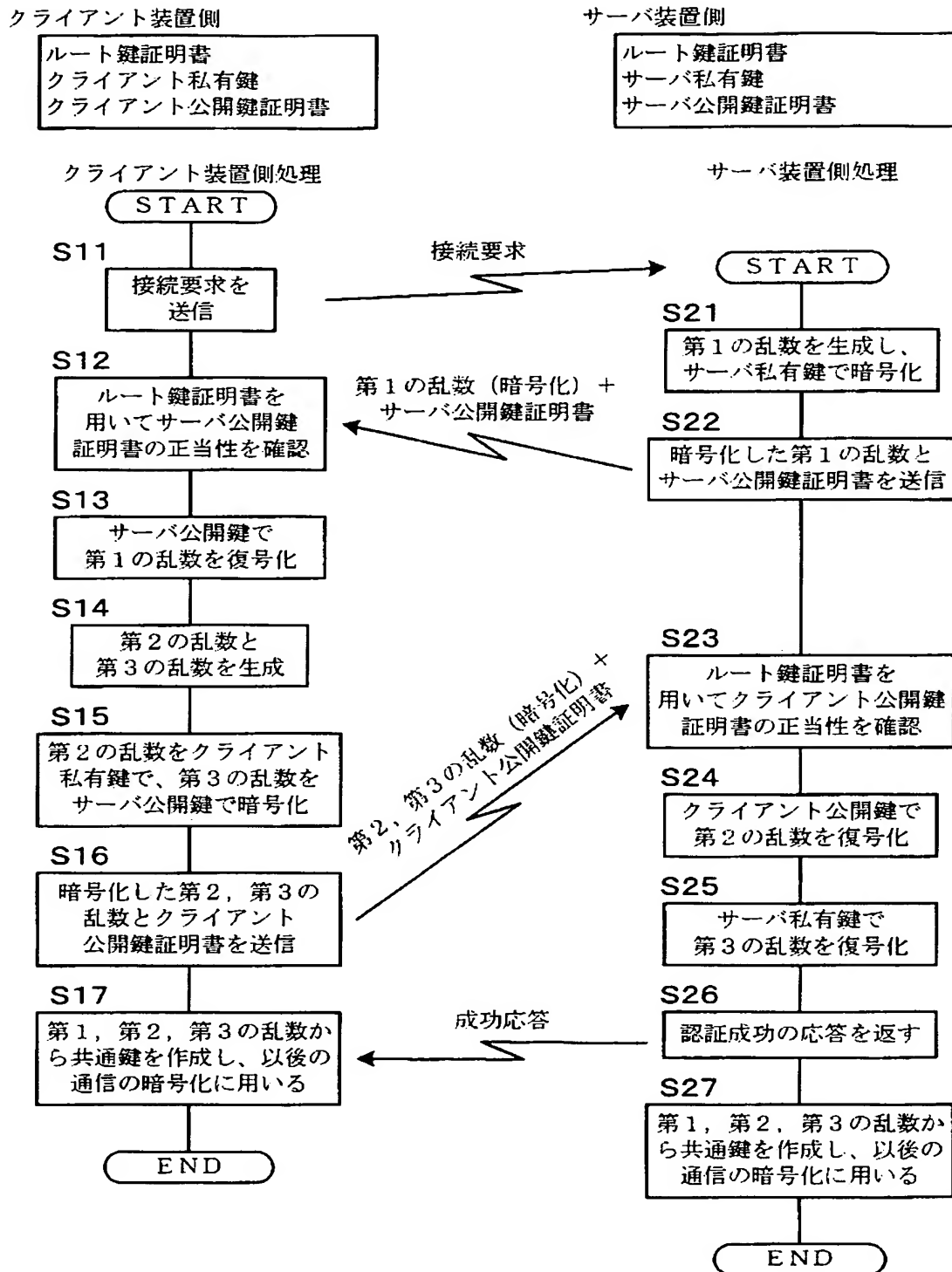
Soap ヘッダ'	書き込み結果送信コマンド'	機種機番1, OK
-----------	---------------	-----------

(b)

受信応答

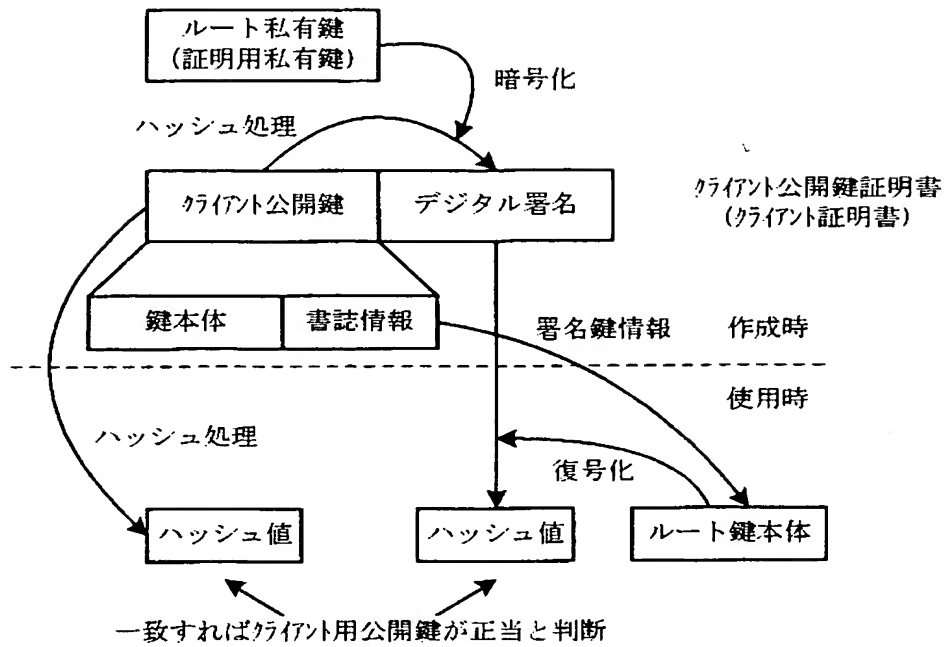
Soap ヘッダ'	書き込み結果応答コマンド'	OK
-----------	---------------	----

【図 24】

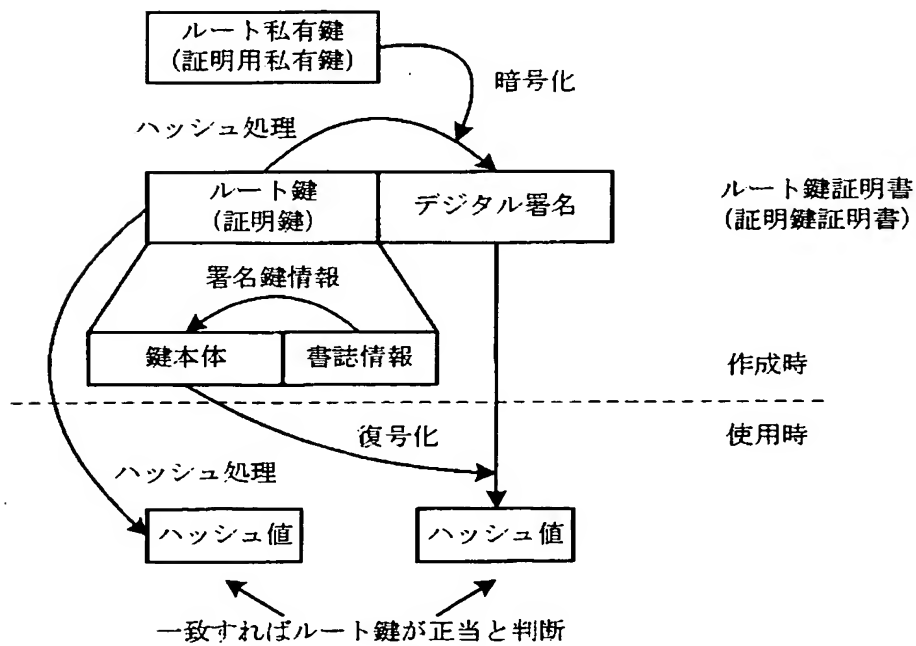


【図 25】

(a)



(b)



【書類名】 要約書

【要約】

【課題】 中央管理装置側が、通信装置と通信する際の認証時に、その通信装置が保守契約したものであるかどうかを正確に判定できるようにする。

【解決手段】 通信端末 150 の CPU は、画像形成装置 100 等の通信装置による SSL 通信時の相互認証に用いる証明書の送信要求にその通信装置の機種機番をその生産台数分だけ付加して証明書管理装置 607 へ通知し、その証明書管理装置 607 からその各機種機番をそれぞれ含む各証明書を受信すると、その各証明書を証明書 DB 154 a に保存した後、上記生産台数分の通信装置のいずれかの機種機番を示すバーコードがバーコードリーダ 141 で読み取られ、そのバーコードによる機種機番が工場端末 160 経由で入力されると、その機種機番に対応する証明書を証明書 DB 154 a から読み出して工場端末 160 により上記通信装置へ送信させ、その通信装置の不揮発性メモリに書き込ませる。

【選択図】 図 10

特願 2003-096240

出願人履歴情報

識別番号

[000006747]

1. 変更年月日

2002年 5月17日

[変更理由]

住所変更

住 所

東京都大田区中馬込1丁目3番6号

氏 名

株式会社リコー